Издается с 1924 года

РАДИО®

8•2015

МАССОВЫЙ ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЖУРНАЛ

"Радиолюбитель"—"Радиофронт"—"Радио"

"Radio" is monthly publication on audio, video, computers, home electronics and telecommunication

УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ: ЗАО «ЖУРНАЛ «РАДИО»

Зарегистрирован Министерством печати и информации РФ 01 июля 1992 г.
Регистрационный ПИ № ФС77-50754

Главный редактор В. К. ЧУДНОВ

Редакционная коллегия:
А. В. ГОЛЫШКО, А. С. ЖУРАВЛЁВ, Б. С. ИВАНОВ, С. Н. КОМАРОВ, А. Н. КОРОТОНОШКО, К. В. МУСАТОВ, И. А. НЕЧАЕВ (зам. гл. редактора), Л. В. МИХАЛЕВСКИЙ, С. Л. МИШЕНКОВ, О. А. РАЗИН, Б. Г. СТЕПАНОВ (первый зам. гл. редактора), В. В. ФРОЛОВ

Выпускающие редакторы: С. Н. ГЛИБИН, А. С. ДОЛГИЙ

Обложка: В. М. МУСИЯКА

Вёрстка: Е. А. ГЕРАСИМОВА

Корректор: Т. А. ВАСИЛЬЕВА

Адрес редакции: 107045, Москва, Селиверстов пер., 10, стр. 1
Тел.: (495) 607-31-18. Факс: (495) 608-77-13
E-mail: **ref@radio.ru**

Группа работы с письмами — (495) 607-08-48
Отдел рекламы — (495) 608-99-45, e-mail: **advert@radio.ru**
Распространение — (495) 608-81-79; e-mail: **sale@radio.ru**
Подписка и продажа — (495) 607-77-28
Бухгалтерия — (495) 607-87-39

Наши платёжные реквизиты:
получатель — ЗАО "Журнал "Радио", ИНН 7708023424,
р/сч. 40702810438090103159
Банк получателя — ОАО "Сбербанк России" г. Москва
корр. счет 30101810400000000225 БИК 044525225

Подписано к печати 17.07.2015 г. Формат 60×84 1/8. Печать офсетная.
Объём 8 физ. печ. л., 4 бум. л., 10,5 уч.-изд. л.
В розницу — цена договорная

Подписной индекс:
по каталогу «Роспечати» — 70772;
по Объединённому каталогу «Пресса России» — 89032;
по каталогу Российской прессы ПОЧТА РОССИИ — 61972.

Отпечатано в ЗАО «ПОЛИГРАФИЧЕСКИЙ КОМПЛЕКС «ЭКСТРА М», 143400, Московская обл., Красногорский р-н, а/м «Балтия», 23 км.
Зак. 15-07-00284.

На страже Солнечного города

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Люди не становятся лучше — только умнее".

Стивен Кинг

Снабдив жителей Солнечного города всем тем, что можно придумать в рамках Интернета вещей (IoT — Internet of Things) и Всеобъемлющего Интернета (IoE — Internet of Everything), и предоставив в их распоряжение всё новые бизнес-модели, использующие вместе с IoT и IoE мобильные и "облачные" решения, нельзя забывать, что всё это сопряжено с большими рисками для информационной безопасности (ИБ). Вот и мы в очередной раз обращаемся к вопросам её обеспечения.

Быстрый рост и распространение технологий IoT и IoE представляются сегодня неизбежными. Многие связанные с этим изменения могут поначалу произойти незаметно для потребителей, но долгосрочный эффект будет исключительно выгодным для всех: и для частных лиц, и для экономики в целом. Ожидаются существенные улучшения в сферах транспорта, экологии, безопасности, реализации концепции подключённых сообществ (например, школ) и т. д. Носимые устройства для мониторинга состояния здоровья и физической активности, "умные" автомобили и системы электроснабжения, подключённые буровые вышки и производственные цеха — всё это лишь начало грядущего переворота в нашем образе жизни, работы, учёбы и отдыха. Соответственно большие перемены уже наступают в здравоохранении, теплоснабжении и производстве, а также в управлении жизненно важными инфраструктурами. Прежде всего, все эти отрасли стремительно "умнеют", для чего инженерам приходится решать целый комплекс задач.

К примеру, чтобы сделать производство "умным", необходимо обеспечить быструю и безопасную интеграцию систем промышленной автоматизации и контроля с бизнес-системами. Необходимо построить единую надёжную конвергентную сеть, которая обхватит производственные и бизнес-подразделения. Необходимо обеспечить полный оперативный контроль цепочки поставок для ускорения обнаружения и устранения проблем с целью снижения времени производственных простоев и повышения эффективности использования оборудования. И много чего ещё необходимо, но прежде всего необходимо обеспечить укрепление информационной безопасности путём контроля доступа к сети, данным и процессам.

Все IoT-устройства постоянно обмениваются информацией со многими другими устройствами, что стремительно увеличивает риски для безопасности. В частности, исследование компании HP показало, что 70 % наиболее часто используемых "умных" приборов, имеющих выход в Интернет, уязвимы, а 80 % устройств подвержены утечке информации в той или иной степени и когда-то уже выдавали личную информацию о своих владельцах, например, логины и пароли, адрес электронной почты, домашний адрес, дату рождения или информацию о кредитной карте.

Внедрение IoT оказывает двойной эффект на информационную безопасность. Ключевые средства IoT разработаны так, чтобы обнаруживать и предотвращать такие угрозы, как утечка данных. Но они же могут использоваться и для того, чтобы предотвращать проникновение злоумышленников в систему с целью хищения данных или, что гораздо опаснее, перехвата управления и причинения ущерба. Недавно британский телеканал BBC провёл эксперимент. Они пригласили суперкоманду из семи специалистов по компьютерной безопасности в дом, напичканный "умными" устройствами. За несколько часов им удалось взломать все до одного устройства. Как отметил один из "взломщиков", больше всего стоит бояться микрофона, подключённого к "умному" телевизору, — с его помощью нетрудно организовать "про-

слушку" дома. Однако многие пользователи даже не задумываются о своей безопасности, полностью доверяясь IoT-девайсам. Поэтому прогнозы аналитиков по поводу бесконечного роста числа IoT-устройств не выглядят такими оптимистичными.

Есть и ещё один дополнительный риск — это отсутствие международных IoT-стандартов. Вопрос, скорее, в последствиях, которые могут наступить в случае взлома M2M-техники, особенно на предприятии или в "умном городе". Впрочем, безопасность — вопрос больше технический и теоретически вполне решаемый. Осталось его решить на разных уровнях безопасности.

Пользователь современной сети связи зачастую использует не только свой терминал, но и виртуальные, мобильные и облачные инфраструктуры. Всё это существенно увеличивает совокупное атакуемое информационное пространство и даёт злоумышленникам возможность сначала скомпрометировать рядовые узлы сети, а затем использовать их как плацдармы для атаки более важных ресурсов и данных.

Стратегии применения IoT неустанно развиваются, и специалистам по сетям и ИБ надо успевать поддерживать безопасность на должном уровне. Очевидно, им следует продумать, как отделить друг от друга различные ресурсы сети и как ограничить между ними ненадлежащие или вредоносные коммуникации. Это жизненно важно для постоянного обеспечения безопасного доступа и применения соответствующих политик, направленных на защиту ценных данных, ограничение горизонтального распространения вредоносного ПО и противодействие сканированию сети.

Правильная сегментация сети может значительно осложнить злоумышленникам поиск и кражу данных. К примеру, лечащему персоналу требуется постоянный, непрерывный доступ к аппаратам искусственного дыхания, внутривенным помпам, системам наблюдения за пациентами. С другой стороны, пациентам и посетителям медицинского учреждения доступна возможность работы, общения и развлечения через Интернет. И именно правильное сегментирование сети может гарантировать, что никто из пациентов или посетителей во время работы в сети не получит намеренно или случайно доступ к данным других пациентов и самого учреждения или даже к важному медицинскому оборудованию. То же самое можно сказать и о современных авиалайнерах, к системам управления которых могут подобраться хакеры, чтобы, например, немного "порулить". Во всяком случае, среди множества версий о недавнем бесследном исчезновении малазийского аэробуса была и такая. Очевидно, что число и разнообразие всевозможных атак будут увеличиваться, и это станет серьёзным испытанием для тех, кто обеспечивает информационную безопасность.

В этой связи крайне интересен приведённый ниже комментарий председателя совета директоров, главного исполнительного директора компании Cisco Джона Чемберса к ежегодному отчёту компании по информационной безопасности: *"На самом деле все компании можно поделить на две категории: уже пострадавшие от хакерских атак и те, что ещё не ведают о том, что они пострадали. В 2014 г. атаки на системы безопасности крупных игроков всех отраслей приобрели характер эпидемии, хотя достоянием гласности становились только самые значительные из них. По данным наших исследований, абсолютно во всех бизнес-сетях есть трафик, ведущий на сайты с вредоносным ПО, а число инцидентов в системах кибербезопасности госструктур США в период с 2010 г. по 2013 г. выросло на 35 %. И пока нет никаких признаков того, что эта тенденция идёт на спад. Наоборот, атаки только учащаются и становятся всё изощрённее. Поэтому вопрос не в том, проникнут ли киберпреступники в наши сети и датацентры, а в том, когда это случится.*

Экономический потенциал IoE в глобальном масштабе составляет 19 трлн долларов США. При этом в эпоху повсеместной связи вопросы безопасности станут вызывать ещё большую озабоченность. Для IoE простого использования имеющихся моделей ИТ-безопасности будет недостаточно. Нужен новый подход к ИБ, необходимы прорывные идеи и инновации. Я призываю современных руководителей со всем вниманием отнестись к тому, о чём пойдёт речь ниже.

При разработке атак злоумышленники рассчитывают на человеческое доверие к системам, приложениям, другим людям и организациям. Поскольку заслуживающих полного доверия сетей и устройств попросту не существует, зачастую, когда дело касается незаконного проникновения, самым слабым звеном оказывается человек. На первый взгляд, проблема может показаться непреодолимой. В действительности же перед бизнесом открывается возможность при разработке стратегии применения технологий и систем защиты использовать решение проблем безопасности как механизм роста. Мы должны помнить об информационной безопасности всегда, до, во время и после атаки.

Чтобы в таких условиях поддерживать высокий уровень доверия со стороны заказчиков, партнёров и сотрудников, каждая компания должна чувствовать свою ответственность за обеспечение ИБ. И хотя, повторяю, безопасных сетей и устройств не существует, стратегия, сфокусированная на главной проблеме обеспечения ИБ — попытках преодоления систем защиты, поможет нейтрализовать действия злоумышленников и обеспечить защиту обширных сетей и развивающейся бизнес-среды.

Хороший лидер не должен давать себе поблажек в оценке собственных систем безопасности. Стоит задаться такими вопросами, как наличие в распоряжении компании средств управления ИБ и качество их тестирования, наладка процесса отчётности, получение необходимой дополнительной информации.

ИБ перестала быть сугубо технологической проблемой — теперь она касается всех. Лидерам промышленности и бизнеса нужно совместно обсуждать потенциальные риски и искать решения для защиты как интеллектуальной собственности, так и финансовых данных.

Чрезвычайно важны также глобальная бдительность и сотрудничество в области анализа информации. В отсутствие общих стандартов градус дискуссий по поводу интернет-безопасности растёт повсеместно. А в таких регионах, как Восточная Европа, где управлению киберпространством уделяют недостаточно внимания, киберпреступность уже процветает. В конце концов, несогласованность подходов к обеспечению информационной безопасности может привести к ограничению потоков данных через межгосударственные границы. Нужен глобальный диалог между правительствами, обществом и частным сектором, который поможет выработать соглашение о способах обеспечения безопасности интернет-экономики. Совместные успехи Комиссии по интернет-технологиям (Internet Engineering Task Force, IETF) и других организаций, занимающихся стандартизацией, позволяют с оптимизмом смотреть в будущее, но решать проблемы управления киберпространством должны сегодняшние лидеры.

Всеобъемлющий Интернет способен преобразовать мир, но чтобы изменения были осмысленными, мы должны задуматься над тем, как сделать так, чтобы каждый мог безопасно использовать открывающиеся возможности. Нужно найти способ, который сделал бы обеспечение информационной безопасности стратегическим механизмом роста не только для каждого отдельно взятого бизнеса, но и для мировой экономики в целом. Если каждый член мирового сообщества посчитает безопасность общим делом, то вместе мы сможем продвинуться на пути к решению технологических и экономических проблем всего человечества".

Несмотря на рост экономических показателей и социальные выгоды, приносимые новыми технологиями, необходимо помнить о возможных негативных последствиях и рисках. Об этом говорится в опубликованном в ноябре прошлого года отчёте Консультативного комитета по связи в системе национальной безопасности США (National Security Telecommunications Advisory Committee, NSTAC). В комитет входят 30 высокопоставленных представителей индустрии телекоммуникаций, которые консультируют президента США по соответствующим вопросам. В отчёте, в частности, говорится: "Остаётся всё меньше времени на то, чтобы обеспечить внедрение технологий IoT максимально надёжным образом и с минимальными рисками. Если наша страна не сделает это, то ей придётся иметь дело с последствиями на протяжении поколений… Осталось всего лишь три года, и уж никак не более пяти лет, на то, чтобы повлиять на степень безопасности применения технологий IoT".

Вместе с тем необходимо совершенствовать защиту всех IoT-приложений, и не только в финансовой сфере. В частности, в отчёте, подготовленном в сенате США, говорится, что мобильные телефоны и такие встроенные системы, как General Motors On Star, могут подключаться к автомобильным системам управления. Среди возможных последствий — "принудительное выполнение транспортным средством внезапных ускорений и поворотов, отключение тормозов, подача звукового сигнала, управление фарами, изменение показателей спидометра и индикатора топлива". На газовой скважине или нефтеперерабатывающем заводе используются не такие каналы связи, как на автомобиле, но и здесь злоумышленники могут проникнуть в систему IoT-управления через уязвимое соединение.

Что же касается модных сегодня "умных городов", то там проблем ожидается ещё больше. Концепция "умного города" в настоящее время широко обсуждается, и масса организаций работает над созданием особых технологий, которые позволят сделать город энергоэффективным, комфортным, экологичным и физически безопасным. При этом вопросы ИБ таких городов остаются на втором плане несмотря на то, что чем больше высоких технологий в городском пространстве, тем выше риск их использования для реализации разнообразных сценариев кибератак. Однако если не подумать о защите заблаговременно, то впоследствии решать возможные проблемы будет гораздо сложнее и затратнее, а город при этом может стать открытым для киберпреступников. Именно поэтому ведущие исследователи и компании, работающие в сфере ИБ (Лаборатория Касперского, IOActive, Bastille и Cloud Security Alliance), объединяют свои усилия и начинают обмениваться экспертными знаниями в рамках международной некоммерческой инициативы Securing Smart Cities, призванной решить проблемы ИБ современных городов. Проект объединит организации, правительства, СМИ, некоммерческие компании и отдельных экспертов, занимающихся разработкой, совершенствованием и продвижением безопасных технологий для городского пользования.

Разумеется, вопросы ИБ обозримого будущего отнюдь не ограничиваются IoT, IoE или растущим внедрением облачных технологий. В феврале текущего года в Стэнфордском университете в Пало-Альто состоялась конференция Белого дома по кибербезопасности и защите потребителей, в которой приняли участие Б. Обама, представители его администрации, главы крупнейших энергетических и интернет-компаний, банков и платёжных систем. Многое из того, что говорилось на этом форуме, может быть экстраполировано на любую развитую страну, довольно далеко зашедшую по пути внедрения Интернета во все стороны жизни государства.

Если говорить коротко, то США собираются взять на себя ответственность за обеспечение безопасности всех 3 млрд пользователей Интернета и 10 млрд подключённых устройств. Безопасность в Интернете официально увязана с военной и энергетической безопасностью, а также экономическим ростом США, ну а хакерские атаки считаются угрозой национальной безопасности.

Директор национального комитета по экономике Джеф Зайнтс призвал частный сектор объединить усилия с государством, чтобы построить лучшую систему кибербезопасности в мире. Если этого не сделать, неэффективная защита станет тормозом в развитии экономики США. Компании несут прямые потери от взломов в десятки миллионов долларов и потенциальные потери в миллиарды долларов из-за кражи разработок и технологий киберворами интеллектуальной собственности — от истребителей до смартфонов. Тут прозвучал более чем прозрачный намёк на Китай и южнокорейские компании.

Кибербезопасность и защита потребителей, по словам Зайнтса, — это две стороны одной медали. Он привёл статистику: девять из десяти американцев считают, что утратили контроль над своими персональными данными, а значит, со временем они могут потерять веру в цифровую экономику США. Более 100 млн аккаунтов было скомпрометировано в результате взломов за прошлый год только в США. Всё это повышает издержки американского бизнеса, поэтому необходимо инвестировать в кибербезопасность системно и агрессивно. При этом Зайнтс заявил, что эти вложения можно превратить из затрат на снижение бизнес-рисков в источник доходов, так как, будучи лучшими в защите информации, США смогут предоставлять защищённые хранилища для неё всему миру, услуги по проведению платежей, банкингу и личным коммуникациям через американские же смартфоны.

Американские компании делают многое, чтобы защитить безопасность своих пользователей и свою репутацию, однако в одиночку они не могут справиться с этим и имеют право ожидать от США решительных действий, если они подверглись взлому. Иными словами, администрация предлагает конгрессу США снова расширить полномочия президента по силовому вмешательству в мире.

Секретарь департамента коммерции Пенни Притцкер, принадлежащая к одной из правящих династий США, сделала обзор полярных точек зрения на право государства распоряжаться персональными данными пользователей. Она, в частности, указала на необходимость обучения молодых специалистов по кибербезопасности. Тем более, что согласно исследованиям PWC, 85 % руководителей компаний беспокоят эти вопросы ("Странно, что не 100%!" — удивилась П. Притцкер), ведь к Интернету в США подключено уже практически всё — от термостатов до тостеров. На вопрос П. Притцкер, уверены ли компании, что инвестируют в безопасность достаточно, участники ответили, что никто не знает, сколько "достаточно". Инвестировать надо, но процесс — бесконечный: сколько бы они ни вкладывали, тех, кто "ломает", — больше, и это надо понимать.

Глава корпорации Apple Тим Кук заявил, что все имеют право на приватность и безопасность. В частности, Apple продаёт лучшие технологии в мире, но никогда и никому не продаёт персональные данные своих пользователей, ни из iCloud, ни из почты, ни из истории браузера. Теперь к этим данным присоединяется информация о состоянии здоровья и финансовых транзакциях, и они тоже не будут переданы никому и никогда. Глава Apple заявил, что компания запрашивает вашу информацию лишь для того, чтобы повысить качество своих услуг. Пользователи сами выбирают, что, как и когда передавать Apple, а что запретить распространять. Как отметили СМИ, при этом в голосе Т. Кука чувствовалась обида, что может быть связано со шквалом критики, который пережила недавно Apple после череды взломов профилей голливудских звёзд. Также Apple обиделась на ритейл за сопротивление Apple Pay, а ведь эта система — самая безопасная, так как уже основана на биометрической идентификации. Преступность в сети растёт очень быстро, и нельзя затягивать с внедрением разработки Apple. Теперь же американскому бизнесу дан чёткий сигнал практически из Белого дома. Всю концовку своего выступления Тим Кук посвятил важности работы администрации президента в области кибербезопасности, так как одной компании, даже такой, как Apple, это не под силу. Apple активно сотрудничает с государством в этом вопросе и сразу же внедряет плоды этого сотрудничества.

Президент Б. Обама начал своё выступление шутками про то, какие у него были пароли. Потом он обратил внимание аудитории на двойственность информационных технологий, которые одновременно дают Америке силу и делают её уязвимой. Например, армия США наиболее технологически развита, однако подвергается угрозам хакеров из России и Китая (впрочем, а что ещё он мог ожидать, если только что его страна впервые решила проводить хакерские атаки на военную инфраструктуру противников в зоне конфликтов, как следует из обновлённой стратегии Министерства обороны США в сфере кибербезопасности). Между тем подвергаются опасности финансовые системы, энергетические сети, здравоохранение, авиационные службы. Одними из самых серьёзных угроз он считает компрометацию данных граждан США, хищение денег онлайн и угрозу безопасности детей.

Далее Б. Обама озвучил следующие принципы безопасности:

— принцип разделения — правительство и бизнес должны работать над обеспечением кибербезопасности вместе, должен быть налажен обмен информацией;

— фокус на сильные стороны — бизнес укрепляет свою защиту и разрабатывает технологии, государство обеспечивает стандарты и их повсеместное внедрение;

— фокус на приватность — обеспечение безопасности и уважение частной жизни;

— стандарты по информированию пользователей о хищении их персональных данных;

— пользователи должны знать, какая их персональная информация собирается и как она будет использована;

— создание объединённого центра борьбы с киберугрозами, компании должны направлять информацию об атаках и делиться наработками по противодействию;

— хабы обмена информацией для ускорения получения данных;

— создание комитета по кибербезопасности;

— инвестиции в биометрическую идентификацию.

Несмотря на то что правительству США, вроде бы, удалось разработать детальную программу деятельности в области Интернета, его безопасности, развития и защиты доминирующего положения своей киберэкономики, консолидировать общество и бизнес, указанных стандартов пока нет, да и в мире всё обстоит не так просто. Ведь весь мир, включая Европу, в соответствии с новой политикой США оказывается на вторых ролях, и любая попытка изменить эту ситуацию будет выглядеть как угроза национальной безопасности этой страны. Таким образом, вектор действий США на ближайшие годы задан чётко, и всем строителям Солнечного города из "интернет-кирпичиков" следует учитывать, что обеспечение ИБ для одной страны может представлять собой потенциальную угрозу ИБ для всех остальных.

По материалам ***Cisco, Gazeta.ru, CNews, vestnik-sviazy.ru, PCWeek, Лаборатория Касперского, newsru.com.***

Вышли в свет новые книги

Телекоммуникационные системы и сети. Учебное пособие в 3-х томах. Том 3. — Мультисервисные сети. — М.: Горячая линия — Телеком, 2015. — 592 с., ил. Под редакцией профессора В. П. Шувалова. Величко В. В., Субботин Е. А., Шувалов В. П., Ярославцев А. Ф. 2-е изд., стереотип. Первое издание вышло в свет в 2005 г.

ISBN 978-5-9912-0484-2

В третьем томе учебного пособия рассмотрены вопросы построения мультисервисных сетей связи (МСС). В компактном виде представлен материал по сетям доступа, транспортным сетям и сетям управления. Приведено описание таких технологий, как Softswitch и MPLS и даны примеры построения сетей на их основе. Пособие содержит раздел по моделированию МСС с использованием аппарата сетей систем массового обслуживания.

Для студентов вузов связи и колледжей, может быть использовано работниками предприятий связи.

Кукк К. И. Спутниковая связь: прошлое, настоящее, будущее. — М.: Горячая линия — Телеком, 2015. — 256 с., ил.

ISBN 978-5-9912-0512-2.

Книга посвящена истории, современному состоянию и перспективам развития систем спутниковой связи, которые в настоящее время являются неотъемлемой и непрерывно растущей частью мирового инфокоммуникационного пространства. В ней дано современное представление о теоретических основах спутниковой связи, а также об аппаратных комплексах — от полезной нагрузки космических аппаратов до характеристик космодромов и средств выведения на орбиты искусственных спутников Земли.

Рассмотрены крупнейшие отечественные и зарубежные системы спутниковой связи с использованием геостационарных и других орбит космических аппаратов. Большое внимание уделяется спутниковому телерадиовещанию и перспективным технологиям спутниковой связи.

Благодаря тому что книга содержит большое количество актуальных справочных материалов, она будет полезна зрелым инженерам, специалистам, студентам радиотехнических и телекоммуникационных факультетов учебных заведений, а также всем тем, кто желает ознакомиться с проблемами спутниковой связи и вещания.

Для широкого круга читателей.

Научно-техническое издательство «Горячая линия — Телеком»
Справки по тел.: (495) 737-39-27, WWW.TECHBOOK.RU

ПРИЗЫ ЖУРНАЛА "РАДИО"

Редакция рассмотрела поступившие письма читателей с купонами журнала "Радио" за 2014 год. В результате наши призы, наборы для самостоятельной сборки **"Автомат световых эффектов на микроконтроллере"**, получат ***Ф. П. Мудров*** (ст. Ардым Пензенской обл.), ***Н. С. Дмитриев*** (г. Канаш, Чувашия), ***В. Н. Фетисов*** (г. Серпухов Московской обл.), ***Н. С. Краснощёков*** (г. Красноярск), ***В. Г. Попсуйко*** (г. Харабали Астраханской обл.).

Поздравляем всех призёров!

Желаем успехов в творчестве!

УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Помните, что журнал "Радио" — радиолюбительский и для радиолюбителей. Мы публикуем статьи по тематикам, интересующим широкий круг читателей. Пишите нам, что Вы хотели бы видеть на страницах журнала, какие темы интересны, а от каких публикаций можно воздержаться. Конечно, мы не гарантируем, что сможем удовлетворить все пожелания, но постараемся их учесть.

Присылайте нам статьи с описаниями своих разработок. Мы рассматриваем всю поступающую почту. В случае положительного решения Ваша статья будет опубликована на страницах журнала "Радио" и сможет в дальнейшем участвовать в конкурсе на лучшую публикацию.

Напоминаем, что конкурс на лучшую публикацию 2015 года продолжается. Приглашаем всех читателей стать заочными членами жюри этого конкурса. Напишите нам, какие, на Ваш взгляд, материалы, опубликованные в журнале "Радио" в 2015 г., заслуживают быть отмеченными премиями. В своих письмах указывайте, пожалуйста, фамилию автора, полное название статьи, номер журнала, в котором она опубликована, а также премию (первая, вторая, третья, поощрительная), которую заслуживает статья. Число указанных материалов не должно превышать восьми. Ваше мнение мы сможем учесть, если Вы отправите письмо не позднее **31 марта 2016 г.** (по почтовому штемпелю). Письмо можно направить и по электронной почте на адрес **mail@radio.ru** с обязательной пометкой в поле "Тема" — "Лучшие публикации 2015 года". По традиции читатели, назвавшие правильно не менее четырёх статей, признанных лучшими, получат наши призы.

Редакция

тел. 608-83-05
Приём статей: mail@radio.ru
Вопросы: consult@radio.ru