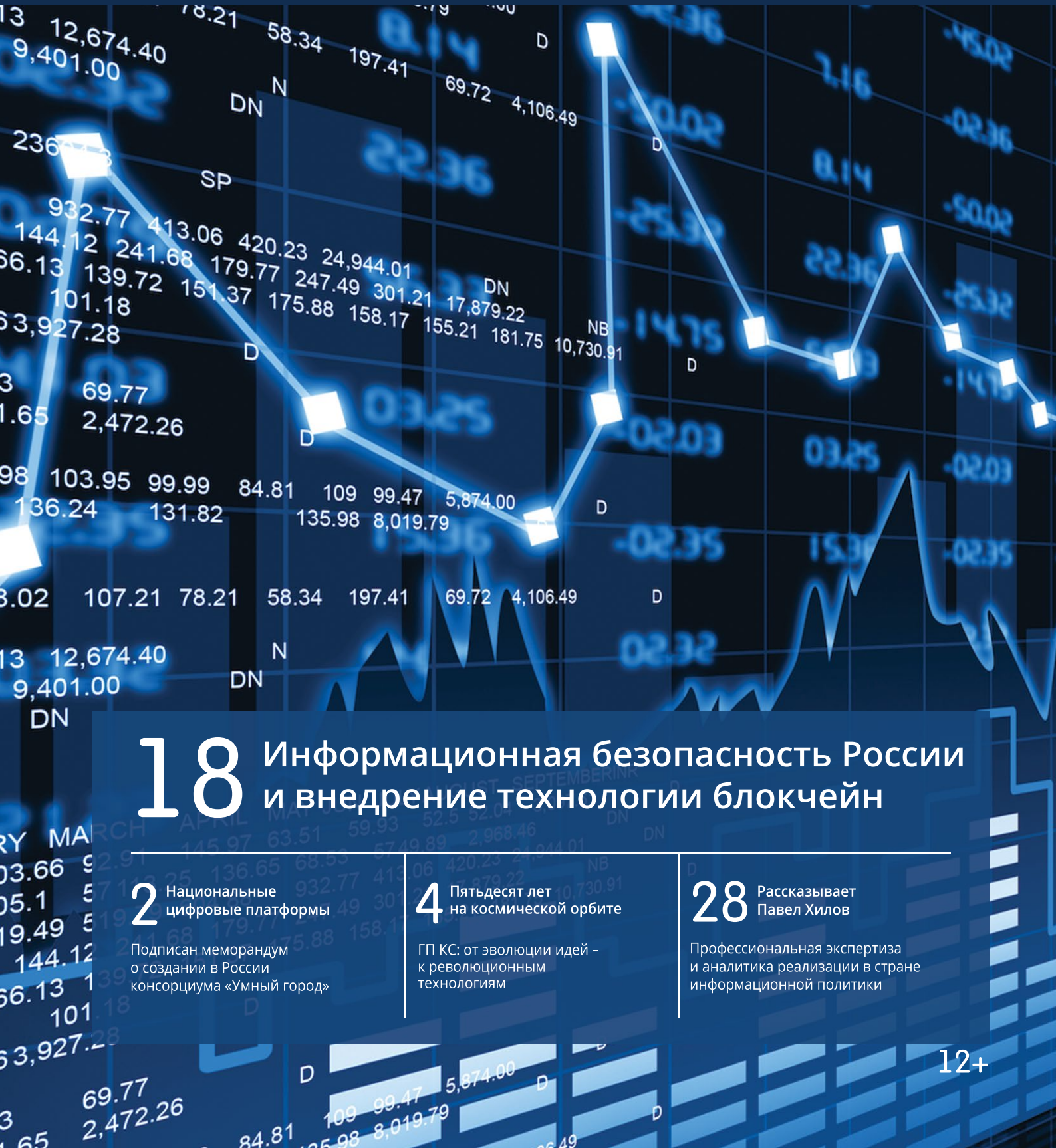
№03 (216), НОЯБРЬ 2017

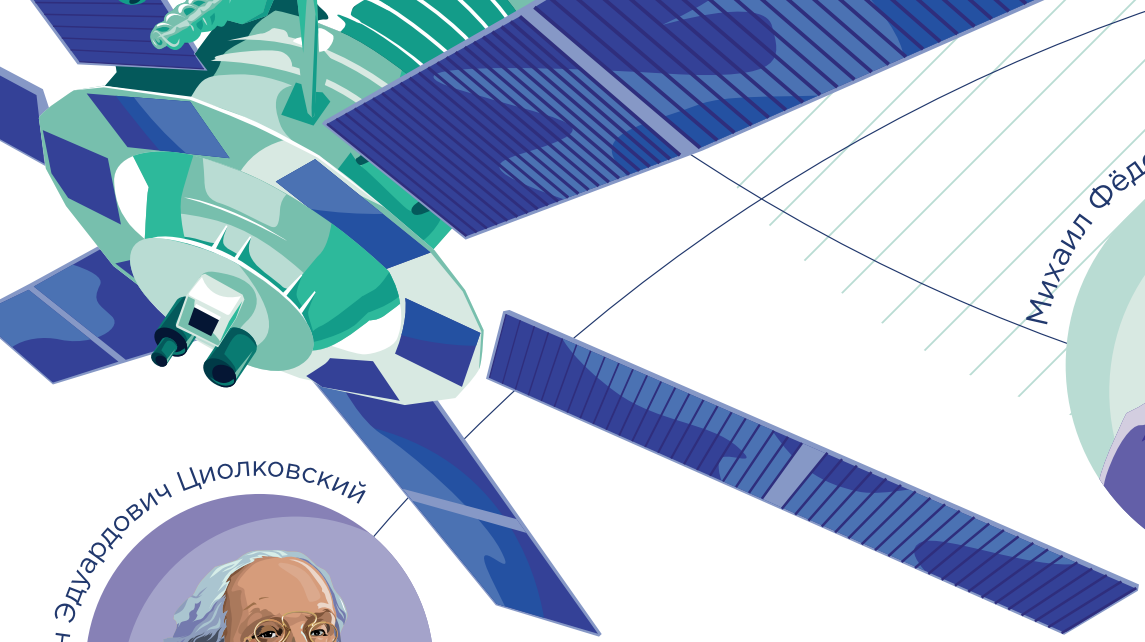
НАУКА • ТЕХНИКА • ИННОВАЦИИ

РАДИОФРОНТ



18 Информационная безопасность России и внедрение технологии блокчейн

12+



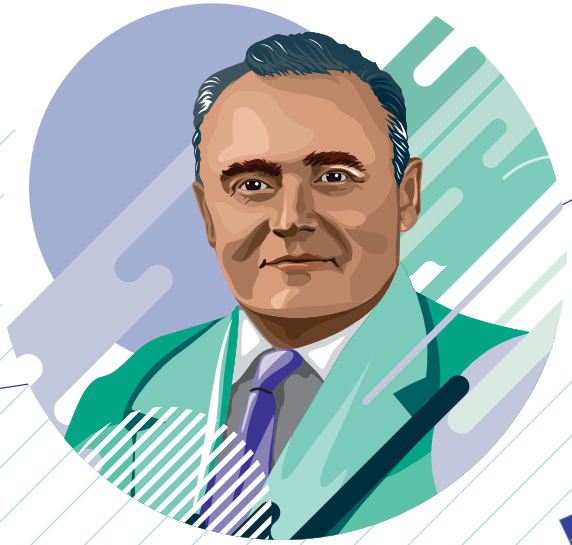
Михаил Фёдорович Решетнёв

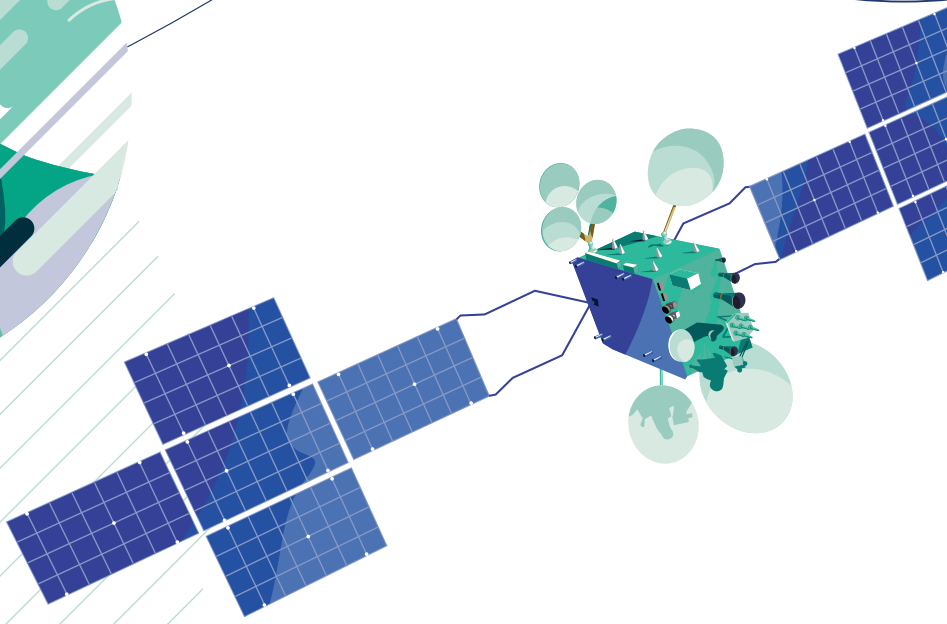
Константин Эдуардович Циолковский

RSCC Космическая связь 50 ЛЕТ НА ОРБИТЕ

"Нет преград человеческой мысли!"

Сергей Павлович Королёв





Общероссийский научно-популярный журнал «РАДИОФРОНТ»
№ 03 (216), ноябрь 2017

Зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, свидетельство о регистрации ПИ №ФС 77 – 70736 от 21.08.2017

Журнал издается с 1930 года.
С 1941 по 2017 год не выходил по независящим от редакции причинам.
Возобновлен в 2017 году.

Учредитель и издатель:
ООО «Радиофронт»

Адрес редакции
Российская Федерация, 127322,
Москва, Огородный проезд, дом 20
Тел. +7 495 9329240
e-mail: a.turbin@fundenergy.ru
www.radiofront.su

Главный редактор
Алексей Турбин

Заместитель главного редактора
Николай Валуев

Над номером работали
Татьяна Валеева
Светлана Селиверстова
Елена Соколова
Дмитрий Кожевников
Олег Дейнеко
Наталья Можаева

Фото в номере
Юрий Ридякин, Алексей Турбин, Николай Валуев, Валерий Стольников, Фотохроника ТАСС, «Объединенная промышленная редакция», личные архивы

Издание подготовлено при участии ООО «Объединенная промышленная редакция»
www.promweekly.ru

Генеральный директор
Валерий Стольников

Отпечатано в типографии «Медиаколор»
Москва, ул. Вольная, 28

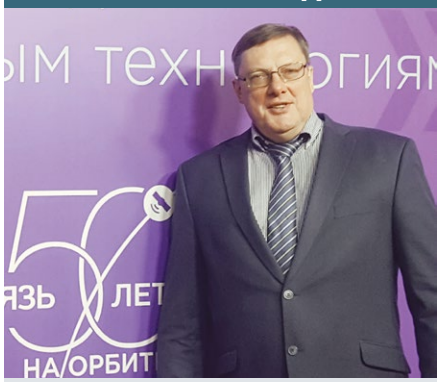
При перепечатке материалов ссылка на издание обязательна

Тираж 5000 экз.

Распространяется бесплатно

СОДЕРЖАНИЕ

СЛОВО ГЛАВНОГО РЕДАКТОРА



УВАЖАЕМЫЙ ЧИТАТЕЛЬ!

Позвольте доложить: казавшаяся иным излишне романтической попытка возродить журнал «РАДИОФРОНТ» вполне может числиться как состоявшаяся. Нас привечают на самых разных важных встречах: и в информационном агентстве ТАСС, и в Зеленограде (конференция SoRuCom, посвященная развитию отечественной вычислительной техники), и в Ярославле (на форуме региональной информатизации «ПРОФ-IT»), и на московском Satcomrus, созванном в ознаменование 50-летия отечественной космической связи, и даже на мероприятиях, приуроченных Посольством Германии к парламентским выборам в этой технически продвинутой стране. Над материалами для журнала вдохновенно корпят лучшие авторы – в том числе в Греции и Швейцарии. Множатся предложения от рекламодателей и ученых, желающих увековечить свои имена на страницах «РАДИОФРОНТА».

Ну и, конечно, (прежний «РАДИОФРОНТ» о таком и мечтать не мог!) мы будем рады приветствовать вас на нашем сайте radiofront.su.

Пользуясь служебным положением, а также пока невысокой периодичностью нашего выхода «в свет», хотел бы первым из коллег-главных редакторов поздравить вас с новым 2018 годом. Давайте не терять друг друга и веру в себя – и все у нас получится!

Алексей Турбин

Михаил Мень,
министр строительства и жилищно-коммунального хозяйства Российской Федерации

«Уже сегодня при строительстве части многоквартирных домов по программам переселения, реализуемым при участии Фонда содействия реформированию ЖКХ, применяются в той или иной степени инновационные технологии «умных домов». Это и приборы регулирования, и системы дистанционного управления тепловыми пунктами и мониторинга показателей, оборудование эффективного использования систем освещения и так далее»...

МЕМОРАНДУМ О СОЗДАНИИ КОНСОРЦИУМА «УМНЫЙ ГОРОД»

Татьяна ВАЛЕЕВА

Фото: «Открытые инновации»

В Москве в ходе Шестого международного форума инновационного развития «Открытые инновации» был подписан Меморандум о создании Национального консорциума развития и внедрения цифровых технологий в сфере городского управления (консорциум «Умный город»). Работа по созданию «умных городов» идет в рамках реализации программы «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства РФ № 1632-р от 28 июля 2017 года. Программа была подготовлена Минкомсвязью России вместе с экспертами и институтами развития.

Одной из основных задач консорциума является создание и реализация концепции «умных городов» на территории РФ. Документ позволит внедрить передовые цифровые технологии в области управления городскими хозяйствами на территории РФ, обеспечить рост конкурентоспособности российских компаний в сфере информационно-коммуникационных технологий (ИКТ) и создать перспективные продукты и услуги для обеспечения конкурентного предложения на рынках цифровизации управления городами и территориями.

Документ подписали замглавы Минкомсвязи России Сергей Калугин, президент компании «Ростелеком» Михаил Осеевский, заместитель генерального директора по развитию и международному бизнесу корпорации «Росатом» Кирилл Комаров, ректор Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (ИТМО) Владимир Васильев и заместитель декана экономического факультета МГУ им. М.В. Ломоносова Сергей Трухачев.

Работа по созданию «умных городов» идет в рамках реализации программы «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства РФ № 1632-р от 28 июля 2017 года. Программа была подготовлена Минкомсвязью России вместе с экспертами и институтами развития.

Замглавы Минкомсвязи России отметил, что повышение эффективности и прозрачности управления городской средой за счет внедрения цифровых технологий является важной задачей для России. «Города – неотъемлемый участник цифровой трансформации экономики. Занимая всего 2% поверхности земли, на них приходится 70% мирового ВВП и 50% населения. В России городское население уже сегодня составляет 74%», – сказал Сергей Калугин.

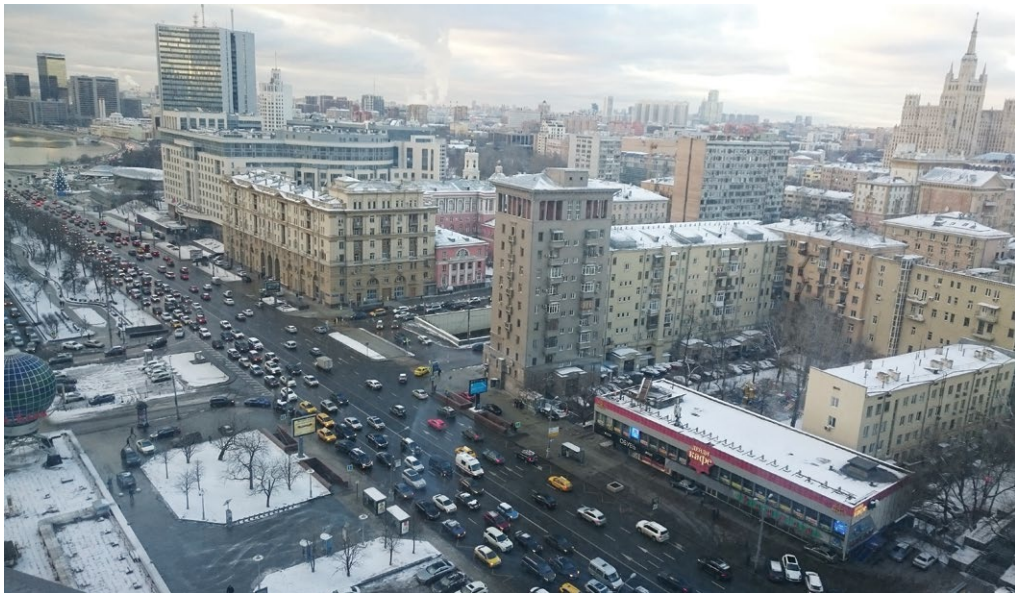
До конца 2017 года планируется определить первые пилотные территории и разработать дорожную карту, включающую мероприятия по применению цифровых платформ управления «умными городами», пилотные проекты по внедрению беспилотного транспорта, повышение прозрачности и эффективности ЖКХ, создание в городах благоприятных условий для развития высокотехнологичных компаний и проектов и другие инициативы.

«Концепция предполагает опережающее развитие 50 городов нашей страны. В них будет сконцентрирован основной капитал цифровой экономики – высококвалифицированные специалисты. Решение такой амбициозной задачи требует объединения усилий и компетенций организаций-лидеров в рамках стратегического консорциума и реализации соответствующих инновационных проектов в интересах почти 50 миллионов жителей нашей страны», – отметил Михаил Осеевский.

До конца 2017 года планируется определить первые пилотные территории и разработать дорожную карту, включающую мероприятия по применению цифровых платформ управления «умными городами», пилотные проекты по внедрению беспилотного транспорта, повышение прозрачности и эффективности ЖКХ, создание в городах благоприятных условий для развития высокотехнологичных компаний и проектов и другие инициативы.

«Мы рады стать участниками такого крупного проекта, который направлен на преобразование городской среды. Уже сейчас многие задачи, стоящие перед правительствами и городскими властями, можно решить именно с применением технологических инноваций, в частности цифровых решений «Росатома», – сказал Кирилл Комаров. – В городах атомной отрасли уже накоплен опыт и компетенции в наукоемких областях, а также работает высококвалифицированный персонал, способный решать сложные и неординарные задачи».

РФ



«КОСМИЧЕСКАЯ СВЯЗЬ»

50 ЛЕТ НА ОРБИТЕ: ОТ ЭВОЛЮЦИИ ИДЕЙ – К РЕВОЛЮЦИОННЫМ ТЕХНОЛОГИЯМ

Станислава ВАСЮТИНСКАЯ

Фото: ФГУП «Космическая связь»

Этот год знаменателен целой серией знаковых «космических» юбилеев. 60 лет назад, 4 октября 1957 года, был запущен в космос «Спутник-1» – первый искусственный спутник Земли. А спустя всего 10 лет, в ноябре 1967 года, в Советском Союзе через космический аппарат «Молния-1» и систему «Орбита» была развернута первая сеть спутникового телевизионного вещания, через которую передавался сигнал из Москвы до тихоокеанского побережья Дальнего Востока. В нашей стране началась эра космической связи, а на базе первой отечественной сети спутникового вещания было образовано уникальное предприятие – ФГУП «Космическая связь» или просто ГП КС.

Юрий Прохоров,
генеральный директор ГП КС

«Сегодня главный результат нашей работы – удовлетворенность пользователей. В условиях открытого рынка и жесткой конкуренции ГП КС успешно работает и занимает лидирующую позицию в домашнем регионе, включающем Россию и страны СНГ»...

За пять десятков лет компания «Космическая связь» прошла непростой путь от станции спутниковой связи до успешного универсального спутникового оператора. И сейчас, используя 12 космических аппаратов связи и вещания и 6 телепортов, ГП КС предоставляет клиентам услуги в 52 странах на всех континентах земного шара.

Начиная с 2000-х на смену спутникам серии «Горизонт» и «Экран» пришли более эффективные космические аппараты (КА) серии «Экспресс». Используя эти КА, ГП КС вступило в жесткую конкурентную борьбу за место в первой десятке крупнейших операторов фиксированной спутниковой связи. Восполнение и модернизация парка космической техники и наземной инфраструктуры позволили ГП КС в несколько раз повысить качество и надежность предоставляемых услуг, а также выйти за границы домашнего региона. Создание предприятием инфраструктуры спутникового непосредственного вещания и широкополосного доступа в Интернет положило начало формированию в нашей стране сегмента продуктов массового потребления в секторе услуг фиксированной спутниковой связи и вещания.

ГП КС смогло преодолеть тяжелый период отказов космических аппаратов на орбите и потери спутников при запусках. Дефицит спутниковой емкости, сложившийся на российском рынке несколько лет назад, преодолен в период 2013-2015 гг. за счет вывода ГП КС на орбиту семи новых спутников.

С 2000 года доступный орбитально-частотный ресурс ГП КС в традиционных C- и Ku-диапазонах увеличился почти в пять раз.

В ходе выставки AfricaCom 2017 (Кейптаун, ЮАР) в присутствии руководителя Федерального агентства связи Олега Духовницкого ГП КС и европейская Chronosat GmbH (Германия) подписали соглашение об увеличении предоставляемого в интересах Chronosat GmbH ресурса космического аппарата ГП КС «Экспресс-АМ7». Достигнута стратегическая договоренность об использовании емкости на космических аппаратах ГП КС на сумму свыше $14 млн в течение ближайших пяти лет.

Рэй Брэдбери,
американский писатель

«В ту ночь, когда Спутник впервые прочертил небо, я глядел вверх и думал о предопределенности будущего. Ведь тот маленький огонек, стремительно двигающийся от края и до края неба, был будущим всего человечества»...

В 2014 году начата эксплуатация спутников с новым для нашей страны Ка-диапазоном частот с высокой пропускной способностью. За 17 лет выручка предприятия выросла в 11 раз, а за последние три года – в два раза.

В соответствии с принятой терминологией, ГП КС является универсальным оператором фиксированной спутниковой связи сегмента B2B. Клиенты компании – сотовые операторы, интеграторы, интернет-провайдеры, операторы сетей VSAT, телерадиокомпании и медиахолдинги, компании, предоставляющие услуги спутникового непосредственного телевизионного вещания, зарубежные и национальные операторы магистральных сетей связи, международные и региональные организации.

В начале 2000-х аналитическое агентство «Euroconsult» давало негативный прогноз дальнейшей операторской деятельности ГП КС на российском рынке. Выход ГП КС на международные рынки не рассматривался вообще. Технологическое и финансово-экономическое сравнение возможностей ГП КС с конкурентами было явно не в нашу пользу. Однако время показало ошибочность этого прогноза.

За прошедшие годы ГП КС создало группировку современных космических аппаратов, зоны покрытия которых охватывают практически весь земной шар. Завоевав доверие европейских пользователей, ГП КС стало наращивать свое присутствие на Ближнем Востоке, в Северной и субэкваториальной Африке, Южной и Юго-Восточной Азии. В этом году компания вышла на рынки Чили и Венесуэлы, Непала и Южной Кореи. Сейчас ГП КС работает в 52 странах мира, и более 40% доходов предприятия поступает от международных продаж.

Еще одним перспективным направлением стало развитие широкополосного доступа на подвижных объектах. В настоящее время компания предоставляет сервисы для морских судов в акваториях Атлантического, Северного Ледовитого и Тихого океанов: это доступ в интернет, прием телевизионных программ, видеонаблюдение и получение метеоданных, телефонная связь. По результатам работы предприятия на меж-

За прошедшие годы ГП КС создало группировку современных космических аппаратов, зоны покрытия которых охватывают практически весь земной шар. Завоевав доверие европейских пользователей, ГП КС стало наращивать свое присутствие на Ближнем Востоке, в Северной и субэкваториальной Африке, Южной и Юго-Восточной Азии. В этом году компания вышла на рынки Чили и Венесуэлы, Непала и Южной Кореи. Сейчас ГП КС работает в 52 странах мира, и более 40% доходов предприятия поступает от международных продаж.

дународных саммитах по вопросам финансирования спутниковой связи в Париже в 2009 и в 2015 годах ГП КС было признано лучшим региональным спутниковым оператором в мире.

Отрасль спутниковой связи, как любая другая, характеризуется цикличностью развития. Начиная с 2014 года, рынок находится в насыщении, повсеместно отмечается избыточность спутникового ресурса в традиционных диапазонах частот. Спутниковые операторы ищут точки роста. В 2016 году доходы мировой индустрии спутниковой связи упали на 1,4% к предыдущему году, в 2015-м совокупные доходы отрасли сократились на 7,3%. Доходы от предоставления инфраструктуры упали в среднем на 3%.

Несмотря на снижение доходов, общий объем потребляемой емкости и пропускной способности продемонстрировали хороший рост (на 12 и 18% соответственно). На положительную динамику спроса оказало влияние появление множества узких зоновых лучей с высокой энергетикой, а также использование технологий гибких полезных нагрузок, которые помогают операторам подстраиваться под изменения спроса. Основными драйверами бизнеса остаются телевизионное вещание, услуги для сотовых операторов, связь на подвижных объектах, корпоративный VSAT, а также ШПД для частных лиц, малых и средних предприятий.

По прогнозам аналитиков, уже в этом году отрасль продемонстрирует стабилизацию ситуации на рынке и, возможно, незначительный рост. По оценкам Euroconsult, суммарная выручка операторов к 2021 году увеличится до $12,4 млрд, а к 2026 – до $15,3 млрд. Прогнозируется, что при стабильном использовании C-/Ku-диапазонов основным драйвером роста доходов будет являться Ka-диапазон. При этом традиционные операторы ФСС столкнутся с новым вызовом – конкуренцией с низкоорбитальными и среднеорбитальными системами фиксированной и подвижной спут-

Сегодня в составе спутниковой группировки ГП КС – 12 космических аппаратов в позициях от 14° западной до 145° восточной долготы. Их зоны обслуживания охватывают всю территорию России, стран СНГ, Европы, Ближний Восток, Африку, Азиатско-Тихоокеанский регион, Северную и Южную Америку, Австралию. Наземная инфраструктура предприятия включает Технический центр «Шаболовка» в Москве, пять Центров космической связи в Центральном регионе, Красноярском и Хабаровском крае и станцию спутниковой связи «Владимир».

До 2025 года ГП КС планирует создание, запуск и ввод в эксплуатацию 5 космических аппаратов на геостационарную орбиту, 4 космических аппаратов на высокоэллиптических орбитах (плюс 1 резервный на земле), а также развитие наземной инфраструктуры. Доступный для использования в сетях спутниковой связи орбитально-частотный ресурс увеличится в 1,7 раза. В настоящее время 2 спутника – «Экспресс-103» и «Экспресс-80» – уже находятся в производстве.

ГП КС считает, что традиционные спутниковые сервисы, такие как телевизионное вещание и магистральные каналы связи, будут по-прежнему востребованы в 10-летней перспективе. Геостационарные спутники идеально подходят для телевидения в нашей стране. Чтобы успешно конкурировать с новыми технологиями вещания, ГП КС планирует сконцентрироваться на создании конвергентных сетей, многофункциональных платформ и интегрированных медиауслуг. Компания планирует и дальше развивать сотрудничество с наземными и сотовыми операторами по услугам резервирования сетей, а также по созданию гибридных сетей, призванных обеспечить потребности современной экономики и пользователей в передаче данных большого объема из любого места.

никовой связи, которые прогнозируют беспрецедентно низкие цены на свои услуги.

В своей Стратегии развития ГП КС концентрируется на нескольких высокотехнологичных направлениях, которые, по нашему мнению, в ближайшее время окажут влияние на структуру рынка спутниковой связи в условиях растущей рыночной конкуренции. Это:

а) реализация новых проектов создания космических аппаратов как на геостационарной, так и на высокоэллиптической орбите, решающих приоритетные задачи фиксированной и подвижной спутниковой связи для государственных и коммерческих заказчиков на территории России, включая Арктический регион;

б) адаптация существующей космической и наземной инфраструктуры предприятия для решения новых задач по обеспечению связью подвижных объектов и развивающегося рынка больших данных, в том числе интернета вещей.

Важным направлением работы ГП КС будет развитие услуг фиксированной и подвижной связи в Арктической зоне с использованием системы связи на высокоэллиптической орбите «Экспресс-РВ». При реализации этого проекта будут созданы условия для предоставления новых видов коммерческих услуг на всей территории России, включая Арктический регион, в части широкополосного доступа на подвижных наземных объектах, в том числе автомобильный, железнодорожный, речной и морской транспорт.

Для сегмента государственных услуг ГП КС видит свою задачу в обеспечении надежности, непрерывности и преемственности развития услуг связи. Одним из перспективных направлений развития спутниковых сервисов будут услуги широкополосной передачи данных, в первую очередь для решения социальных задач и обеспечения доступа к сети Интернет для частных лиц. Эту работу ГП КС планирует осуществлять в партнерстве с операторами конечных услуг в секторе B2C.

Для сегмента государственных услуг ГП КС видит свою задачу в обеспечении надежности, непрерывности и преемственности развития услуг связи. Одним из перспективных направлений развития спутниковых сервисов будут услуги широкополосной передачи данных, в первую очередь для решения социальных задач и обеспечения доступа к сети Интернет для частных лиц. Эту работу ГП КС планирует осуществлять в партнерстве с операторами конечных услуг в секторе B2C.

Мобильная передача данных, HD, IoT, «умные» города и сельское хозяйство, электронное здравоохранение, онлайн-банкинг, связь на транспорте – доступ к частотному ресурсу определяет работу огромного количества компаний из самых разных секторов экономики.

В июле 2017 года утверждена подготовленная Минкомсвязью Программа «Цифровая экономика Российской Федерации», в рамках которой ГП КС планирует свое участие в направлениях:

- нормативное регулирование. Специалисты ГП КС обладают уникальными знаниями и опытом, которые позволяют выступать в качестве экспертов по созданию гармоничной нормативно-правовой базы в области спутниковой связи и вещания для обеспечения необходимых условий развития цифровой экономики. Важным направлением работы является представление интересов РФ на международном уровне с целью создания единой цифровой среды;

- кадры и образование. ГП КС планирует продолжить работу по сотрудничеству с отраслевыми российскими вузами для подготовки нового поколения специалистов для отрасли спутниковой связи;

- формирование исследовательских компетенций и технических заделов. Работа ГП КС в кооперации с российскими исследовательскими институтами и ведущими отечественными производителями космической техники нацелена на разработку и внедрение в проекты ГП КС инновационных идей и технологий;

- информационная инфраструктура. ГП КС предлагает использовать спутниковые сети связи в удаленных и труднодоступных регионах Российской Федерации для обеспечения широкополосного доступа к сети интернет для населения, лечебно-профилактических учреждений, образовательных учреждений, органов власти и местного самоуправления, включая спутниковое резервирование каналов.

РФ

Михаил Осеевский,
президент и председатель правления ПАО «Ростелеком»

«Построенные в рамках проекта УЦН оптические линии связи мы планируем использовать и для других проектов, включая подключение медучреждений. Мы сейчас тестируем решение, позволяющее с использованием оптики, которая пришла в небольшие населенные пункты, предоставлять услуги мобильной связи. Думаю, что тестирование должно завершиться успешно, и тогда у нас появится возможность предложить совершенно другой сервис жителям, в этом необходимость есть».

ТРЕХСТОРОННИЙ СОЮЗ ПРОТИВ ЦИФРОВОГО НЕРАВЕНСТВА

В рамках реформы универсальных услуг связи (УУС) и программы устранения цифрового неравенства в Москве в Сколково подписано трехстороннее соглашение о сотрудничестве с Новосибирской областью. В настоящий момент трехсторонние соглашения о сотрудничестве подписали уже 47 субъектов Российской Федерации.

Наталья МОЖАЕВА

Фото: Минкомсвязь РФ

Цель соглашения – развитие телекоммуникационной инфраструктуры и комплексных государственных информационных систем на территории Новосибирской области. Одним из основных направлений сотрудничества является устранение цифрового неравенства и обеспечение равных возможностей для всех жителей регионов в использовании современных услуг связи, включая высокоскоростной доступ в интернет.

Документ подписали министр связи и массовых коммуникаций Российской Федерации Николай Никифоров, президент компании «Ростелеком» Михаил Осеевский и временно исполняющий обязанности губернатора Новосибирской области Андрей Травников. В рамках соглашения современными услугами связи будет обеспечено свыше 300 населенных пунктов области.

Согласно подписанному документу в 279 населенных пунктах Новосибирской области, где проживают от 250 до 500 человек, будут установлены точки доступа, предоставляющие бесплатный широкополосный доступ в интернет без ограничений по объему переданной или полученной информации на скорости не менее 10 Мбит/с. Еще в 24 населенных пунктах области, где проживают свыше 500 человек, планируется модернизация местной и внутризоновой сети электросвязи, которая позволит предоставлять современные услуги связи, в том числе доступ к скоростному интернету. Подписанное трехстороннее соглашение позволит максимально быстро реализовать план строительства каналов связи и снять все возможные административные барьеры на пути реализации договора.

Распоряжением Правительства РФ № 437-р от 26 марта 2014 года единым федеральным оператором универсального обслуживания назначена компания «Ростелеком». 13 мая 2014 года был подписан десятилетний договор между Федеральным агентством связи и «Ростелекомом» об условиях оказания УУС. Для реализации программы устранения цифрового неравенства должно быть построено около 215 тысяч километров волоконно-оптических линий связи. 1 августа 2017 года отменена плата за использование высокоскоростным интернетом с использованием точек доступа, построенных в рамках проекта по устранению цифрового неравенства.

РФ

ОПЫТ CYBERSECURITY MALAYSIA

Предлагаем вниманию читателей журнала «РАДИОФРОНТ» интервью Дато Хаджи Амирудина Бен Абдель Вахаба (Dato' Dr. Haji Amirudin Bin Abdul Wahab) – генерального директора государственной малазийской технической службы CyberSecurity Malaysia, обеспечивающей, в кооперации с другими органами исполнительной власти, информационную безопасность в стране. Корреспондент беседовал с доктором Амирудином Бен Абдель Вахабом на московской ИБ-конференции BIS Summit.

– В чем задача CyberSecurity Malaysia – защита граждан, компаний, обеспечение государственной IT-безопасности?

– CyberSecurity Malaysia – государственное ведомство, специализирующееся на предоставлении технических услуг. Оно помогает правительству следить за электронной безопасностью страны. Мы работаем под руководством министерства технологий и инноваций и тесно взаимодействуем с национальным советом по безопасности Малайзии. Мы работаем и с гражданами, и с частным сектором, и с государственными организациями, предоставляя им техническую поддержку. Какую именно, зависит от их запроса.

– Т.е. вы не спецслужба?

– Нет, но мы предоставляем услуги любым правительственным службам, включая специальные.

– Сколько сотрудников в вашем аппарате?

– Около трехсот. Надо отметить, что мы предоставляем определенные услуги компаниям на коммерческих условиях. Государственные службы, специальные в том числе, мы обслуживаем бесплатно, поскольку основное финансирование CyberSecurity Malaysia получает от государства.

– Сколько лет работает CyberSecurity Malaysia?

– Уже 20 лет, с 1997 года. Сначала организация называлась CERT (Computer Emergency Response Team). Позже она полу-

чила название MyCERT (Malaysia CERT). В 2006 году государство приняло национальную политику обеспечения кибербезопасности, и в соответствии с ней мы получили нынешний мандат на оказание технической помощи тем, кто в ней нуждается. Круг наших обязанностей и функций расширился. В 2007-м организация прошла ребрендинг, она стала называться CyberSecurity Malaysia и в этом статусе существует по сей день.

– В какой мере проблемы кибербезопасности, которыми вы занимаетесь, специфичны именно для вашей страны?

– По большей части киберугрозы, которым в настоящее время подвергнуты все страны, с точки зрения технологии являются общими, одинаковыми. Это киберпреступность – прежде всего мошенничество, шпионаж и т.н. «hacktivism», хакерская активность, а еще распространение вредоносного ПО. С такими угрозами имеют дело многие страны мира.

Однако у нас в Малайзии есть особая тревога по поводу некоторых видов контента, и в этом отличие от других стран, особенно западных. Когда я говорю о «некоторых видах контента», то имею в виду контент подрывного характера, или диффамацию, т.е. клевету. В западном мире высказывания подобного рода часто не преследуются, они считаются проявлением свободы вообще и свободы слова в частности. Но в малазийском контексте это может стать причиной беспорядков, привести к нарушению общественной безопасности. Поэтому распространение таких высказываний преследуется по закону, который запрещает диффамацию и подрывную деятельность и действует вне киберпространства, т.е. вне зависимости от того, где и как запрещенная информация распространяется.

Мы верим в международное сотрудничество. У себя в Азиатско-Тихоокеанском регионе, а также среди стран Организации исламского сотрудничества мы активно работаем для этого. В дополнение к международным программам сотрудничества мы также участвуем в двусторонних программах. Это помогает реагировать на инциденты, когда мы становимся объектом внешней атаки.

В Малайзии все, что связано с подрывной деятельностью и диффамацией, входит в сферу ответственности королевской полиции. Она осуществляет оперативную работу, а мы предоставляем для этого техническую помощь и поддержку. У полиции есть полномочия вести расследования, а у CyberSecurity Malaysia – технические знания, необходимые для расследований в киберпространстве.

– А профилактическая работа по блокированию нежелательного контента?

– У нас есть регулятор – Malaysian Communications and Multimedia Comission, MCMC. Она несет ответственность за весь сектор ИКТ, лицензирует деятельность операторов связи и интернет-провайдеров. Решение о блокировании тех или иных ресурсов принимает MCMC, а мы, если это необходимо, оказываем MCMC техническую поддержку.

– Чему CyberSecurity Malaysia приходится уделять наибольшее внимание?

– У нашей организации есть колл-центр, он называется «Cyber 999», туда может обратиться любой пользователь Интернета. «Cyber 999» работает под надзором одного из наших департаментов, MyCERT. Информация обо всех киберинцидентах, поступающая в «Cyber 999», классифицируется по девяти категориям. Среди этих девяти типов инцидентов на первые три места постоянно выходят мошенничество (fraud), незаконные вторжения («hacktivism») и вредоносное ПО (malware). Есть и другие типы инцидентов, напри-

CyberSecurity Malaysia взаимодействует с некоторыми российскими компаниями, например, InfoWatch, и целым рядом других, которые даже открыли представительства в Куала-Лумпуре. Два года назад мы подписали договор с Академией информационных систем, АИС, и в рамках этого взаимодействия я неоднократно приезжал в Россию, чтобы прочесть лекции. Меня представили ряду людей. Так получилось, что я стал приезжать в Россию чаще. Убежден, что мы можем сотрудничать с любой страной, и Россия – одна из них.

мер, киберпреследование людей («cyberharassment»). Но на мошенничество приходится почти 50%, во всяком случае не менее 40% всех обращений, поступающих в колл-центр. Как следствие, именно проблема кибермошенничества имеет наибольший вес среди задач, стоящих перед CyberSecurity Malaysia.

Что касается нежелательных проникновений, то они представляют собой проявления хакерской деятельности, «hacktivism». Вредоносное ПО тоже серьезная проблема, недавний пример – эпидемия компьютерных вирусов-шифровальщиков WannaCry и Petya. Мотивы у вирусописателей могут быть самые разные, от шпионажа до всего что угодно.

Некоторые преступные организации рассматривают Малайзию как плацдарм для атаки на другие страны – через ботнеты.

– Какова динамика?

– Уже 5-6 лет эта картина не меняется. Однако мы исходим из того, что в ближайшее время проблемы, порождаемые киберпреступностью, станут еще более острыми. Такой вывод мы делаем потому, что видим: преступников мотивирует стремление получить незаконную финансовую выгоду.

– Киберпреступники не считаются с национальными границами, но государства вынуждены сотрудничать в борьбе с ними. Как у вас это получается?

– Мы верим в международное сотрудничество. У себя в Азиатско-Тихоокеанском регионе, а также среди стран Организации исламского сотрудничества (объединяет более 50 государств. – *Прим. ред.*) мы активно работаем для этого. В дополнение к международным программам сотрудничества мы активно участвуем в двусторонних программах. Это помогает реагировать на инциденты, когда мы становимся объектом внешней атаки.

Рассмотрим в качестве примера уже упомянутую эпидемию WannaCry. Когда мы стали получать информацию из Европы, где разворачивалась атака вируса-шифровальщика, то сразу стали обмениваться информацией о развитии ситуации и опытом ее преодоления, чтобы лучше реагировать на угрозу. Внутри же страны CyberSecurity Malaysia вступила в активное взаимодействие с государственными организациями с целью минимизировать ущерб.

Наша реакция включала также сотрудничество с компаниями – мы получили инструменты и ресурсы, чтобы предотвратить последствия распространения вируса, свести ущерб к минимуму. Это были как местные малазийские компании, так и иностранные, работающие в Малайзии.

– Не могли бы вы привести конкретный пример взаимодействия на государственном уровне – скажем, если атаковавший вас хакер находится в Норвегии, сколько времени займет связаться с коллегами, и пойдут ли они вам навстречу?

– Тут все зависит от доверия и мер, принимаемых для его укрепления. В отношениях между странами АТР – а они очень тесные – такое доверие есть, и если произойдет атака с территории другой страны региона, ее правительство нам поможет. Нам предоставят всю информацию, которой располагают власти.

Европа и Америка – это регионы, где нам предстоит укреплять международное сотрудничество. Мы убеждены, что такое сотрудничество следует наладить во всем мире. Например, в следующем году, в июне, мы в Малайзии будем принимать конференцию FIRST – Forum of Incident Response and Security Teams. FIRST – международная организация со штаб-квартирой в США, она объединяет CERT-структуры различных стран. Проведение конференции реализует нашу стратегию сближения с другими государствами для совместного противодействия киберугрозам.

– Входит ли в сферу ваших интересов безопасность инфраструктуры?

– Инфраструктура – зона ответственности регулятора, т.е. MCMC. Но мы предоставляем им консультации и поддержку по вопросам, связанным с кибербезопасностью.

– Связность национальных сетей, их устойчивость под, как говорят в России, «неблагоприятным внешним воздействием» – это тоже дело регулятора?

– Как я уже сказал, в 2006 году Малайзия сформулировала и привела в действие политику кибербезопасности. Реализация этой политики координируется

на самом высоком уровне, комитетом национальной безопасности. Выделяются 10 секторов критически важной инфраструктуры. Одним из них является сектор ИКТ. По каждому из секторов назначен регулятор. Соответственно, когда речь идет о вопросах национальной безопасности, регулятор передает их на решение в комитет национальной безопасности. Наша роль состоит в том, чтобы обеспечить технической помощью и консультацией всех регуляторов. Таким образом, мы работаем на линии пересечения всех секторов, а не только в секторе ИКТ.

– Не кажется ли вам потенциально опасной ситуация, когда национальные правительства не управляют Интернетом? Я имею в виду, например, контроль над корневыми DNS-серверами.

– Управление Интернетом – проблема глобального масштаба. Странам бывает непросто договориться на эту тему, поскольку у каждой свои собственные интересы в сфере безопасности. Чтобы найти решение, потребуется время на бюрократические процедуры, не говоря уже о политических вопросах. Надо сказать, что интерпретация этих вопросов может отличаться от страны к стране. Мы считаем, что лучше применять мягкий подход – делать акцент на развитии доверия и расширении контактов.

– Государства, возможно, и смогли бы договориться, но где им это сделать? Они – лишь одни из стейкхолдеров в ныне действующей модели управления Интернетом, наряду с университетами и отдельно взятыми экспертами.

– Это непростая проблема, потому что централизованного контроля у Интернета нет.

– Ну почему же? IANA – это место, откуда теоретически можно «выключить» любой корневой домен, и государства не смогут на это повлиять.

– Мир отличается от того, каким он был раньше, теперь в нем нет единой точки координации. Могу повторить: мы убеждены, что все вопросы надо решать через укрепление доверия и сотрудничество всех заинтересованных сторон, в их общих интересах, несмотря на то что задача эта простой не будет.

Мир отличается от того, каким он был раньше, теперь в нем нет единой точки координации. Могу повторить: мы убеждены, что все вопросы надо решать через укрепление доверия и сотрудничество всех заинтересованных сторон, в их общих интересах, несмотря на то что задача эта простой не будет.

– Используете ли вы собственные технологии? Россия сейчас решает задачу импортозамещения ПО.

– Мы предоставляем услуги. Разработка технологий, R&D – этим занимаемся не мы, а другие ведомства. Что касается инструментов, то используем и те, которые разработаны в Малайзии, и зарубежные. Мы комбинируем их, составляем из них собственные решения, новые средства, которые позволяют бороться с новыми угрозами.

Разработкой собственных технических средств в области ИКТ занимается национальное исследовательское агентство MIMOS, это их обязанность – создавать отечественные средства и вести инновационные разработки для защиты критической национальной инфраструктуры.

– Российские программные продукты используете?

– Да, например, продукты «Лаборатории Касперского». Мы открыты для использования любого ПО.

Что касается национальной безопасности, наша задача состоит в том, чтобы провести техническую оценку и сертификацию средств, используемых для ее обеспечения. У нас есть лаборатория для исследования и оценки ИКТ-продуктов с точки зрения их безопасности, и мы можем по результатам исследования выдавать сертификаты информационной безопасности.

CyberSecurity Malaysia взаимодействует с некоторыми российскими компаниями, например, InfoWatch и целым рядом других, которые даже открыли представительства в Куала-Лумпуре. Два года назад мы подписали договор с Академией информационных систем, АИС, и в рамках этого взаимодействия я неоднократно приезжал в Россию, чтобы прочесть лекции. Меня представили ряду людей. Так получилось, что я стал приезжать в Россию чаще. Убежден, что мы можем сотрудничать с любой страной, и Россия – одна из них.

– Есть ли контакты с российским правительством?

– С правительственными организациями в России у нас контактов нет.

– Какое достижение CyberSecurity Malaysia вы считаете важнейшим?

– Мы гордимся тем, что вносим вклад в глобальную кибербезопасность. Малайзия в рейтинге Global Cybersecurity Index, GSI, ежегодно составляемом Международным союзом электросвязи, уже два раза подряд занимает третье место (Российская Федерация – на 10-м. – *Прим. ред.*) среди 164 стран.

РФ

ДЛЯ ЗАЩИТЫ И БЕЗОПАСНОСТИ

ПРОИЗВОДИТЕЛЯМ ЭЛЕКТРОНИКИ И ИТ-КОМПАНИЯМ ПРЕДСТАВИЛИ РИЦ «СЭЙФНЭТ»

Надежда ЗИМИНА, Санкт-Петербург

Фото: Ассоциация разработчиков и производителей электроники

На территории Технопарка Санкт-Петербурга российские разработчики программного обеспечения и производители электроники провели обсуждение перспектив сотрудничества с Региональным инжиниринговым центром «Развитие рынка систем безопасности информационных и киберфизических систем» (РИЦ «СэйфНэт») кластера «Развитие информационных технологий, радиоэлектроники, приборостроения, средств связи и инфотелекоммуникаций г. Санкт-Петербурга».

Создание РИЦ «СэйфНэт» – одно из основных направлений совместной работы НП «РУССОФТ» и Ассоциации разработчиков и производителей электроники (АРПЭ), в числе учредителей которой – холдинг GS Group. Руководство РИЦ «СэйфНэт» и президент НП «РУССОФТ» Валентин Макаров презентовали представителям GS Nanotech (предприятие в составе GS Group), Luxoft St. Petersburg и других компаний возможности и стратегию развития создаваемого центра.

ОАО «НПО Цифровые Телевизионные Системы». Монтаж выводных компонентов на печатные платы

Формирование РИЦ «СэйфНэт» инициировано НП «РУССОФТ» и рабочей группой SafeNet Национальной технологической инициативы на бюджетные средства Санкт-Петербурга. Цель – производство и тестирование программно-аппаратных решений в области безопасности, компонентов доверенной среды для киберфизических систем. Первоочередные задачи центра – развитие прототипа доверенной среды SafeNet, создание хабов квантовых коммуникаций, построение ЦОД с квантовой защитой, создание прототипа защищенной связи для Интернета вещей, формирование профессиональных экспертных сообществ в этой сфере.

«Проект инжинирингового центра был изначально ориентирован на новую парадигму развития науки и промышленности России, на национальные технологические

инициативы, в частности в сфере SafeNet, которая пронизывает собой все остальные инициативы и является основной платформой, поддерживающей киберфизическую безопасность. Концепция рынка SafeNet НТИ направлена на достижение российскими компаниями значимой доли мирового рынка безопасности, а также на обеспечение национальной технологической безопасности через поддержку ключевых решений НТИ. Дорожная карта SafeNet предполагает создание к 2035 году адекватной национальной платформы безопасности информационных и киберфизических систем, покрывающей потребности в этой области во всех рынках НТИ. Российский сегмент рынка SafeNet должен занять не менее 3-5% от мирового объема. РИЦ «СэйфНэт» создается для индустрии, и мы надеемся, что он будет эффективно поддерживать компании региона», – рассказал участникам встречи директор РИЦ «СэйфНэт» Антон Колошин.

Технический директор РИЦ «СэйфНэт» Андрей Иванов отметил, что в мире появляются новые устройства, которые могут подвергаться угрозам и требуют проактивных и максимально защищенных систем управления. Такие системы должны обеспечивать коридоры безопасности, например, движения беспилотников, носимой медицины, «умных домов» и «умных городов», «индустрии 4.0», процессов передачи и хранения гостайны, банковских транзакций. «С точки зрения физической структуры мы представляем это в виде защищенной 5g-сети, включающей различные базовые станции. Что касается интеллектуальной части, нам необходимы доверенные операционные системы, системы обработки и хранения данных, системы виртуализации, сервисы и приложения, работающие в комплексе и обеспечивающие высокий уровень безопасности», – добавил спикер.

Создание инжинирингового центра в Санкт-Петербурге для производства и тестирования комплексных решений в области SafeNet, разработка доверенной среды для построения защищенной инфраструктуры SafeNet – одно из основных направлений совместной работы НП «РУССОФТ» и Ассоциации разработчиков и производителей электроники (АРПЭ).

ОАО «ДжиЭс Нанотех».
Процесс монтажа кристалла на подложку

«В РИЦ «СэйфНэт» будут создаваться прототипы доверенных программно-аппаратных систем и отрабатываться методики их проектирования. Совместно с НП «РУССОФТ» мы будем продвигать эти методики среди заказчиков, отвечающих за создание ИТ-инфраструктуры. Добиться высокого уровня доверенности невозможно, находясь в зависимости от закрытых проприетарных решений зарубежных компаний. Эта задача требует тесного и открытого сотрудничества заказчиков с разработчиками аппаратных и программных компонентов систем», – прокомментировал исполнительный директор АРПЭ Иван Покровский.

«Инжиниринговый центр – перспективная площадка для сотрудничества, которая позволит нам расширить деловые контакты, привлечь новых партнеров и заказчиков. GS Group сможет предложить собственные решения в области безопасности как на аппаратном, так и на программном уровнях – полностью российского производства, разработанные, изготовленные и собранные в центре микроэлектроники GS Nanotech. Среди них – микропроцессоры по технологии «система-в-корпусе», препятствующие несанкционированному доступу к контенту, твердотельные накопители для рабочих станций, СХД, data-центров, системы условного доступа и другие разработки. Объединившись с другими участниками РИЦ «СэйфНэт», мы сможем создавать еще более масштабные и комплексные решения для защиты информации мирового уровня», – прокомментировал генеральный директор GS Nanotech Евгений Масленников.

Президент НП «РУССОФТ» Валентин Макаров призвал участников рынка – разработчиков и производителей программного и аппаратного обеспечения консолидировать усилия для развития рынка SafeNet: «РИЦ «СэйфНэт» располагает инновационными технологиями, среди которых квантовые коммуникации, СХД, биоидентификация, а также имеет поддержку отраслевых кооперации, например АРПЭ. Мы можем уже сейчас в ускоренном режиме проводить ОКР. Центр дает компаниям, имеющим решение, возможность превратить его в готовый продукт. Однако для эффективной работы, развития отрасли и завоевания мирового рынка нам необходима более масштабная кооперация, которая позволит вовлечь всех участников в процесс создания доверенной среды и обеспечения национальной технологической безопасности».

НЕ СТАРЕЮТ ДУШОЙ ВЕТЕРАНЫ

Александр РОМАНОВ

Техническое переоснащение ТАСС в соответствии с новейшими достижениям науки и техники, постоянное совершенствование технологий передачи, обработки и классификации информации – эти вопросы были в центре внимания встречи ветеранов и сотрудников крупнейшего российского информационного агентства. Она прошла 5 ноября в главном офисе ТАСС и собрала около 40 бывших ответственных работников агентства, многие из которых ныне занимают руководящие посты в творческих объединениях, бизнесе, газетах и журналах России.

Участники встречи ветеранов ТАСС: легендарный спортивный журналист Всеволод Кукушкин, освещавший 11 Олимпийских игр, и Михаил Беглов, много лет работавший корреспондентом в США, а затем возглавивший Редакцию аудиовизуальной информации ТАСС. Опережая время на десятилетия, это подразделение в 80-е годы научилось транслировать сообщения ТАСС на экраны советских телевизоров, а также вести электронные базы данных.

«Очевидно и плодотворно стремление руководства ТАСС, отметившего свой 113-й день рождения, к активному внедрению инновационных достижений, к постоянному расширению охвата общественно важной информацией отечественных и зарубежных аудиторий, – отметил на встрече действительный государственный советник РФ третьего класса, бывший корреспондент ТАСС в Хельсинки и Виндхуке (Намибия) Алексей Турбин. – Очевидно, что такие встречи весьма полезны и желанны и в человеческом, и в производственном плане. Ведь большинство собравшихся в агентстве были не только свидетелями, но и активными участниками внедрения в ТАСС компьютерной техники, открывшей принципиально новые возможности для журналистской работы».

«Именно благодаря компьютеризации начала 80-х годов в нашем агентстве была создана беспрецедентная для тех лет система передачи и обработки информации, охватившая практически весь мир, – отметила приветствовавшая участников встречи заместитель начальника отдела ТАСС Светлана Лопатина. – Не сомневаюсь, что опыт наших старших товарищей важен для агентства и сейчас: тассовцы не стареют душой, они рады нынешним успехам агентства, уверенно лидирующего по цитируемости в материалах, посвященных событиям в Российской Федерации».

Встреча в главном офисе ТАСС совпала по времени с работой выставки «Главные кадры. ТАСС открывает архивы». Она стала результатом успешного осуществления инновационного проекта по оцифровке богатейшего фотоархива агентства: отсканировано и систематизировано свыше 850 тыс. ценнейших изображений. Для выставки в Центральном выставочном зале «Манеж» были отобраны около тысячи фотографий, отражающих знаковые события XX века.

Генеральный директор ТАСС С. Михайлов открывает выставку «Главные кадры»

Многолетняя сотрудница справочно-информационной службы ТАСС Елена Райкерус в обновленном ньюсруме агентства

«Мы искренне благодарны руководству ТАСС, в первую очередь генеральному директору Сергею Михайлову, за отличную подготовку этой содержательной и долгожданной встречи, которая, как мы надеемся, станет традиционной», – отметил Алексей Турбин, с гордостью продемонстрировавший коллегам номера обновленного журнала «РАДИОФРОНТ».

РФ

Светлана Лопатина,
заместитель руководителя отдела сопровождения пользователей Департамента информационных технологий ТАСС

«Именно благодаря компьютеризации начала 80-х годов в нашем агентстве была создана беспрецедентная для тех лет система передачи и обработки информации, охватившая практически весь мир. Не сомневаюсь, что опыт наших старших товарищей важен для агентства и сейчас: тассовцы не стареют душой, они рады нынешним успехам агентства, уверенно лидирующего по цитируемости в материалах, посвященных событиям в Российской Федерации».

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

МЫ ДОЛЖНЫ ПРОГНОЗИРОВАТЬ УГРОЗЫ, АКТИВНО РЕАГИРОВАТЬ НА НИХ, РАЗВИВАТЬ НАЦИОНАЛЬНУЮ ПРОИЗВОДСТВЕННУЮ БАЗУ

Валерий СТОЛЬНИКОВ

Фото: Пресс-служба Президента РФ, ТАСС

Вопросы информационной безопасности, противодействия киберпреступности, развития информационной инфраструктуры государства и бизнеса становятся в последнее время все более актуальными и все чаще звучат на самом высоком уровне. Например, они стали главной темой прошедшего под председательством Владимира Путина в октябре в Кремле расширенного заседания Совета безопасности, а также встречи в Сочи, которая была посвящена новым электронным финансовым инструментам.

Владимир Путин, Президент Российской Федерации

«Очевидно, что устойчивая работа информационных систем, средств коммуникации и связи, их защищенность имеют для страны стратегическое значение. Это важный фактор обеспечения суверенитета, обороноспособности, безопасности государства, эффективного развития экономики, социальной сферы, государственного управления на базе передовых, в том числе цифровых, технологий»...

Начальник Генерального штаба Вооруженных Сил – первый заместитель министра обороны Валерий Герасимов, мэр Москвы Сергей Собянин

Открывая расширенное заседание Совета безопасности, Владимир Путин, в частности, отметил: «Очевидно, что устойчивая работа информационных систем, средств коммуникации и связи, их защищенность имеют для страны стратегическое значение. Это важный фактор обеспечения суверенитета, обороноспособности, безопасности государства, эффективного развития экономики, социальной сферы, государственного управления на базе передовых, в том числе цифровых, технологий».

Владимир Путин напомнил, что тема развития и безопасности информационной инфраструктуры рассматривалась на заседании Совета безопасности три года назад – в октябре 2014 года, когда в том числе были определены ближайшие и перспективные задачи. «И за прошедшее время, конечно, многое сделано для обеспечения надежной работы информационной инфраструктуры, особенно это касается государственных органов», – подчеркнул Президент РФ.

Успешно действуют федеральные органы, наделенные полномочиями контроля в этой сфере. Имею в виду Федеральную службу по техническому и экспортному контролю, а также ФСБ, которая обеспечивает государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы; активно работают и специалисты Роскомнадзора...

Также было отмечено, что в декабре 2016 года была утверждена Доктрина информационной безопасности России, а с 1 января 2018 года вступает в силу Федеральный закон о безопасности критической информационной инфраструктуры России. Таким образом, считает глава государства, заложен правовой фундамент для дальнейших практических шагов на этом направлении. Также он отметил: «Успешно действуют федеральные органы, наделенные полномочиями контроля в этой сфере. Имею в виду Федеральную службу по техническому и экспортному контролю, а также ФСБ, которая обеспечивает государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак

Председатель Государственной Думы Вячеслав Володин, председатель Правительства Дмитрий Медведев

на информационные ресурсы; активно работают и специалисты Роскомнадзора».

Между тем на расширенном заседании было сказано, что нужно учитывать повышение уровня угроз в информационном пространстве, число рисков увеличивается, а негативные последствия разного рода кибератак носят уже не локальный, а действительно глобальный характер и масштаб. Например, в результате распространения вируса «Вонна Край» в мае-июне этого года пострадали информационные ресурсы в 150 странах мира, в том числе и в России. «Внешнее вторжение в электронные системы в сфере обороны и госуправления, жизнеобеспечивающей инфраструктуры и финансов, утечка электронных документов могут обернуться самыми тяжелыми последствиями» (В. Путин).

Было сказано также, что ряд стран уже фактически поставили информационные технологии на военную службу: формируют свои кибервойска, а также активно используют информационное поле для ослабления конкурентов, продвижения своих экономических и политических интересов, решения геополитических задач в целом, в том числе в качестве фактора так называемой мягкой силы.

«В этой связи, – заявил Владимир Путин, – мы должны четко представлять тенденции развития

Руководитель Администрации Президента Антон Вайно

Ряд стран уже фактически поставили информационные технологии на военную службу: формируют свои кибервойска, а также активно используют информационное поле для ослабления конкурентов, продвижения своих экономических и политических интересов, решения геополитических задач в целом, в том числе в качестве фактора так называемой мягкой силы.

глобальной информационной сферы, прогнозировать потенциальные угрозы и риски. И главное – наметить дополнительные меры, которые позволят нам не просто своевременно выявлять угрозы, а активно реагировать на них».

На расширенном заседании Совета безопасности было обозначено, на чем в первую очередь необходимо сконцентрировать усилия.

Первое – совершенствование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России. В том числе это касается механизмов взаимодействия ее ведомственных сегментов.

Второе – повышение защищенности информационных систем и сетей связи государственных органов с усилением персональной ответственности руководителей за обеспечение информационной безопасности.

Третье – максимальное снижение рисков, связанных с объективной необходимостью использовать иностранные программы и телекоммуникационное оборудование. В этой связи – последовательная реализация проектов и программ импортозамещения, которые осуществляются в стране, а также создание дополнительных мер поддержки и стимулирования отечественных производителей, укрепления потенциала и повышения конкурентоспособности российских компаний.

Четвертое – повышение безопасности и устойчивости работы инфраструктуры российского сегмента интернета без каких-либо ограничений доступа граждан к ресурсам глобальной сети, выстраивания тотальных барьеров и фильтров. «Необходимо строго соблюдать и уважать конституционное право на получение и распространение информации» (В.Путин).

Пятое – активное содействие созданию системы международной информационной безопасности, развитие сотрудничества с партнерами на глобальных и ре-

Полномочный представитель Президента в Уральском федеральном округе Игорь Холманских, директор Федеральной службы войск национальной гвардии – главнокомандующий войсками национальной гвардии Виктор Золотов, губернатор Санкт-Петербурга Георгий Полтавченко

Сергей Шойгу, министр обороны Российской Федерации

«Особняком встал вопрос по кибербезопасности. Здесь у нас очень широкое поле. Эту угрозу я сегодня уже могу назвать кибероружием – оно, конечно, все ближе и ближе к понятию «оружие массового поражения»...

гиональных площадках, таких как ООН, БРИКС, ШОС, АТЭС, ОДКБ, СНГ и других, проводить межведомственные консультации и переговоры. Очевидно, что, объединив усилия, мы сможем более эффективно бороться с современными угрозами.

На тему мер повышения безопасности интернета Владимир Путин высказался конкретно и предметно: «Как и в других демократических странах, мы должны бороться с теми, кто использует информационное пространство для пропаганды радикальных идей, оправдания терроризма, экстремизма, решительно пресекать попытки размещения материалов, угрожающих безопасности нашего государства, общества в целом и отдельных граждан. Вы знаете, в этом году законодательно усилена ответственность за организацию сайтов, призывающих детей и подростков к суициду. Наши правоохранительные органы и спецслужбы стали гораздо чаще выявлять и пресекать деятельность вербовщиков в террористические группировки, в том числе в ряды запрещенной в России ИГИЛ и в другие подобные организации. Так же жестко в рамках закона нужно действовать и в отношении других лиц и групп, использующих интернет, информационное пространство в преступных целях.

Криптовалюты: бить или не бить?

Примечательно, что за неделю с небольшим до расширенного заседания Совета безопасности Владимир Путин провел в Сочи совещание по вопросу использования цифровых технологий в финансовой сфере и внедрения инновационных финансовых инструментов. В этом совещании приняли участие помощник Президента Андрей Белоусов, министр финансов Антон Силуанов, председатель Центрального банка Эльвира Набиуллина, заместитель главы Центробанка Ольга Скоробогатова, генеральный директор компании Qiwi Сергей Солонин.

На этом совещании Владимир Путин отметил, что данная тема «актуальна не только для нашей страны, не только для России, но, наверное, становится актуальной уже и для всего мира. Имею в виду внедрение цифровых технологий в финансовой, банковской сфере; использование инновационных финансовых инструментов».

На совещании было отмечено, что современные технологии в банковской сфере открывают, безусловно, новые возможности для организаций и граждан, делают удобнее хозяйственную деятельность и повседневную жизнь тоже. Большую популярность, как известно, приобретают и уже

Министр финансов Антон Силуанов, заместитель председателя Центрального банка Ольга Скоробогатова

получили виртуальные деньги (криптовалюты), которые в некоторых странах становятся полноценным платежным средством, а также инвестиционным активом.

Владимир Путин обозначил принципиальный подход к данной теме: «Мы должны использовать преимущества, которые дают новые технологические решения в банковской сфере. Вместе с тем использование криптовалют несет и серьезные риски».

Среди рисков были названы следующие:

– возможность отмывания капиталов, полученных преступным путем;

– возможность ухода от налогов;

– возможность финансирования преступных групп, в том числе терроризма;

– создание платформы для распространения мошеннических

схем, жертвами которых могут быть рядовые граждане.

При этом поскольку криптовалюты выпускаются неограниченным кругом анонимных субъектов, их покупатели могут невольно оказаться вовлеченными в противоправную деятельность. Еще один очевидный риск состоит в том, что по криптовалютам не существует обеспечения. В случае сбоя системы или «надувания пузырей», как сейчас иногда модно говорить, по ним не будет юридически ответственного субъекта.

Известно, что многие страны ищут подходы к тому, как регулировать обращение криптовалют, только начинают создавать необходимые законодательные условия, законодательную нормативную базу. По мнению участников совещания в Сочи, России нужно, опираясь на международный опыт, выстроить такую регуляторную среду, которая позволит систематизировать отношения в этой сфере, защитить, безусловно, интересы граждан, бизнеса, государства, дать правовые гарантии для работы с инновационными финансовыми инструментами.

Однако, напомнил Владимир Путин, «при этом важно не нагородить лишних барьеров, разумеется, а создать необходимые условия для дальнейшего развития и совершенствования национальной финансовой системы».

Пять поручений

Главным итогом сочинского совещания по вопросу использования цифровых технологий в финансовой сфере стал ряд поручений, которые утвердил Президент Российской Федерации.

Всего было сформулировано пять президентских поручений в рамках реализации программы «Цифровая экономика Российской Федерации». А именно:

1. Правительству Российской Федерации совместно с Банком России обеспечить внесение в законодательство Российской Федерации изменений, предусматривающих:

а) определение статуса цифровых технологий, применяемых в финансовой сфере, и их понятий (в том числе таких, как «технология распределенных реестров», «цифровой аккредитив», «цифровая закладная», «криптовалюта», «токен», «смарт-контракт»)

УЩЕРБ ОТ УТЕЧЕК ВЫРОС В РАЗЫ

По данным Аналитического центра InfoWatch, в первом полугодии 2017 года в мире было обнародовано в СМИ и иных открытых источниках 925 случаев утечки конфиденциальной информации, что на 10% превышает число утечек данных за аналогичный период 2016 года. Объем скомпрометированных в результате утечек в январе-июне 2017 года записей персональных (ПДн) и платежных данных, включая номера социального страхования, реквизиты пластиковых карт и иную критически важную информацию, увеличился по сравнению с первым полугодием 2016 года почти в восемь раз – с 1,06 млрд до 7,78 млрд записей. Общий объем скомпрометированной в 2016 году информации в мире составлял всего около трех миллиардов записей.

Резкое увеличение объема потерянной чувствительной информации в первом полугодии 2017 года произошло в результате 20 мегаутечек (от 10 млн записей), на которые пришлось 98% пострадавших записей ПДн и финансовых данных. По сравнению с аналогичным периодом прошлого года в распределении утечек по типам данных на 20% увеличилась доля платежной информации и симметрично сократилась доля ПДн.

Причиной 58% утечек в мире стали внутренние нарушители в организации. Существенно возросло среднее число пострадавших записей: в расчете на одну утечку в результате внешнего воздействия приходилось 13,6 млн записей (по сравнению с 2,4 млн в 2016 году) и 4,5 млн записей – на каждую утечку, допущенную по вине внутреннего нарушителя (0,8 млн в 2016 году).

«С начала 2017 года мы фиксируем в мире многократный рост объема скомпрометированных данных, увеличение «мощности» утечек, от которых страдает все больше чувствительной информации, – сказал аналитик ГК InfoWatch Сергей Хайрук. – С развитием цифровой экономики вопросы информационной безопасности переросли отраслевые рамки и широко обсуждаются на самом высоком уровне. Сама тема утечек информации становится все более прозрачной, и это должно позитивно сказаться на общем уровне культуры информационной безопасности. Даже в России пострадавшие орга-

исходя из обязательности рубля в качестве единственного законного платежного средства в Российской Федерации;

б) установление требований к организации и осуществлению производства, основанного на принципах криптографии в среде распределенных реестров («майнинг»), включая регистрацию хозяйствующих субъектов, осуществляющих такую деятельность, а также определение порядка ее налогообложения;

в) регулирование публичного привлечения денежных средств и криптовалют путем размещения токенов по аналогии с регулированием первичного размещения ценных бумаг.

2. Банку России совместно с Правительством Российской Федерации:

а) представить предложения:

– по созданию на базе Банка России специальной регулятивной площадки («сэндбокс») для апробации инновационных финансовых технологий, продуктов и услуг до установления правил регулирования отношений, связанных с их применением на финансовом рынке;

– по формированию единого платежного пространства государств – членов Евразийского экономического союза с применением новых финансовых технологий, в том числе технологии распределенных реестров.

«Мы должны четко представлять тенденции развития глобальной информационной сферы, прогнозировать потенциальные угрозы и риски. И главное – наметить дополнительные меры, которые позволят нам не просто своевременно выявлять угрозы, а активно реагировать на них»...

Владимир Путин

Cryptoleaders и РАКИБ

В продолжение идей сочинского совещания ближе к концу октября в Москве прошла первая встреча российского криптосообщества Cryptoleaders, тон на которой задавал Советник Президента России Герман Клименко.

В ходе дискуссии на встрече главными вопросами стали международное регулирование криптовалют, правовой статус технологии блокчейн и основанных на ней операций. По мнению Германа Клименко, перед государством стоит вопрос создания условий, при которых криптовалюта перестанет нести риски, касающиеся незаконного оборота финансовых средств. Для проработки инициатив в этой области создана Российская ассоциация криптовалют и блокчейна (РАКИБ). Одной из задач РАКИБ является разработка предложений для законопроекта, который определит само понятие криптовалюты и смежных с ней операций, а также регуляторику этих процессов. В рамках встречи криптосообщества состоялась также презентация ряда проектов, в частности – интеллектуальной системы поддержки принятия врачебных решений «Третье мнение».

РФ

низации начинают рассчитывать ущерб, который был нанесен им в результате той или иной утечки. Чтобы минимизировать эти риски, необходим комплексный подход к информационной безопасности предприятий, включая средства защиты от внешних и внутренних угроз».

Доля утечек данных с неправомерным доступом к информации, включая злоупотребление правами доступа и внутренний шпионаж, составила менее 8% от общего числа случаев. Неквалифицированные утечки, которые не сопряжены с превышением прав доступа и использованием данных в целях мошенничества, были зафиксированы в 84% случаев.

В первом полугодии 2017 года по сравнению с аналогичным периодом 2016 года увеличилась доля утечек через сетевой канал и электронную почту. Снизились доли утечек данных в результате кражи/потери оборудования, с использованием съемных носителей и бумажных документов. Большая часть утечек наиболее «ликвидной» платежной информации пришлась на два канала – в 45% случаев финансовые данные передавались в сеть Интернет через браузер или облачное хранилище, еще 44% таких утечек произошли с использованием корпоративной электронной почты.

Чаще всего утечки происходили в организациях медицинской сферы, реже всего – в сегменте промышленности и транспорта. Наибольший объем скомпрометированных записей пришелся на сектор высоких технологий, включая интернет-сервисы и крупные порталы. Утечки из госорганов составили около16% от общего объема скомпрометированных записей.

В первом полугодии 2017 года наибольший интерес злоумышленники проявляли к банкам и компаниям высокотехнологичного сегмента. В этих отраслях более 50% утечек ПДн носили умышленный характер.

«Коммерческие и государственные сервисы обрабатывают все больше данных в электронном виде, и такие данные крайне ликвидны, – отметил Сергей Хайрук. – Сектор высоких технологий очень сильно подвержен утечкам информации, как и финансово-кредитная сфера. Эти отрасли вызывают наибольший интерес со стороны злоумышленников – в них большая часть данных была скомпрометирована умышленно. И это как раз те сегменты, которые являются драйверами цифровой экономики, с развитием которой нужно уделять особое внимание вопросам регулирования и информационной безопасности процессов цифровой трансформации».

ВЫСОКАЯ АКТУАЛЬНОСТЬ

ОТЕЧЕСТВЕННАЯ «ВЕРСИЯ» БОРЬБЫ С КИБЕРАТАКАМИ

Александр КОМАРОВ

«Глава Microsoft заявил, что КНДР стоит за кибератакой WannaCry». «Власти Великобритании обвинили Иран в кибератаке на парламент». «Министр обороны Польши заявил об «отражении кибератаки» из-за рубежа». «Это сумасшествие»: в России ответили на обвинения США в использовании софта «Лаборатории Касперского» для шпионажа». Все это – заголовки «молний» информационных агентств, вышедших на ленты всего за два дня в середине октября. При этом вполне очевидно, что темы, затронутые в них, по сути однородны: речь идет о реальных угрозах, которые в наш неспокойный век гибридных противостояний таят в себе агрессивные действия IT-группировок, направленные против определенных компаний, отраслей промышленности, а то и против целых стран.

Под кибератакой понимается осмысленное действие в рамках кибервойны, понимаемой как противоборство или противостояние в кибернетическом пространстве, в том числе компьютерное противостояние в интернете. Кибератаки бывают направлены прежде всего на дестабилизацию компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран и государств, которые полагаются на интернет в повседневной жизни. Межгосударственные отношения и политическое противостояние часто находит продолжение в интернете в виде кибервойны и ее составных частей: вандализме, пропаганде, шпионаже, непосредственных атаках на компьютерные системы и серверы и так далее. Кибератаки представляют в наши дни большую опасность, чем когда-либо в обозримом прошлом, отмеченном развитием IT-технологий.

Утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. Доктрина информационной безопасности Российской Федерации определяет обеспечение информационной безопасности нашей страны как один из приоритетов государственной политики, как «осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления».

Утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. Доктрина информационной безопасности Российской Федерации определяет обеспечение информационной безопасности нашей страны как один из приоритетов государственной политики, как «осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления».

Поставляемая ООО «Версия» система NT40E3-4-PTP

Устанавливаемые «Версией» платы идеально подходят для высокоскоростных приложений захвата и анализа данных, с возможностью воспроизведения записанных сегментов трафика. С их помощью осуществляется сетевой мониторинг, анализ и фильтрация, а также сетевое тестирование.

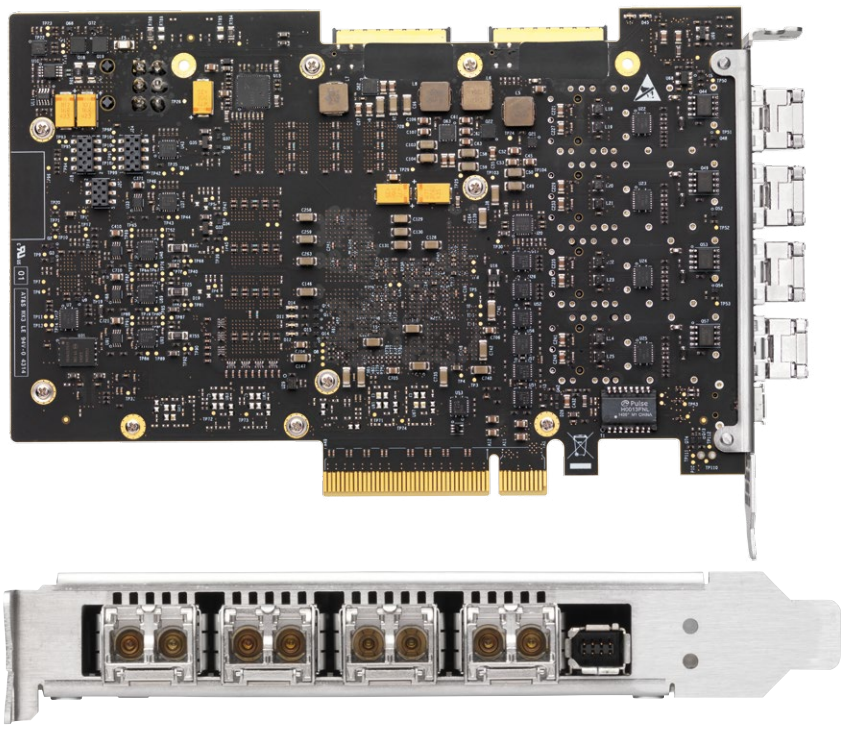
Это определение обретает повышенную актуальность ввиду того, что цифровая эпоха неумолимо движется вперед, практически вся информация оцифровывается. Наши удостоверения, медицинские документы, финансовая информация, а также общественная инфраструктура, железнодорожные системы, электростанции и т.д. теперь доступны и управляются по сети – и, следовательно, становятся потенциальной мишенью авторов кибератак.

В этой связи высокую актуальность приобретает оборудование, поставляемое российской компанией ООО «Версия». Компания является одним из крупнейших поставщиков высокотехнологичных решений в области телекоммуникаций. Она обладает богатым опытом внедрения специализированных высокоскоростных плат захвата трафика (сетевых адаптеров, «акселераторов») с программируемой логикой (ПЛИС), которые предназначены для гарантированного захвата всего объема передаваемого трафика в сети на скорости до 200 Гбит/с. Также они позволяют проводить преданализ проходящего трафика аппаратными средствами в режиме In-line и хранение данных для последующей пост-обработки в среде вышестоящих приложений.

Данное решение обеспечивает гарантированный захват и передачу всего объема данных в Систему хранения данных (СХД) на полной линейной скорости интерфейса адаптера, без потери пакетов.

Идеологической основой адаптера является технология ПЛИС (Программируемая логическая интегральная схема), которая позволяет высокоэффективно решать сложные задачи, даже на скоростях выше 100 Гбит/с. Именно единая логика позволяет безболезненно масштабировать решения в будущем и переходить на более скоростные потоки, не предпринимая фундаментальных изменений в программном обеспечении приложений.

Немаловажной особенностью «акселераторов» является наличие вставки высокопрецизионной (до 4 нс) аппаратной метки, присваиваемой каждому пакету, поступившему на порт адаптера. Это позволяет адаптеру объединять весь массив поступающих данных с разных портов в единый логический поток и значительно облегчить дальнейшую обработку. Наличие высокоточной аппаратной временной метки открывает путь к особо требовательным секторам, где любая погрешность или задержка оказывают прямое влияние на экономику, финансы, безопасность или эффективность работы соответствующей структуры.

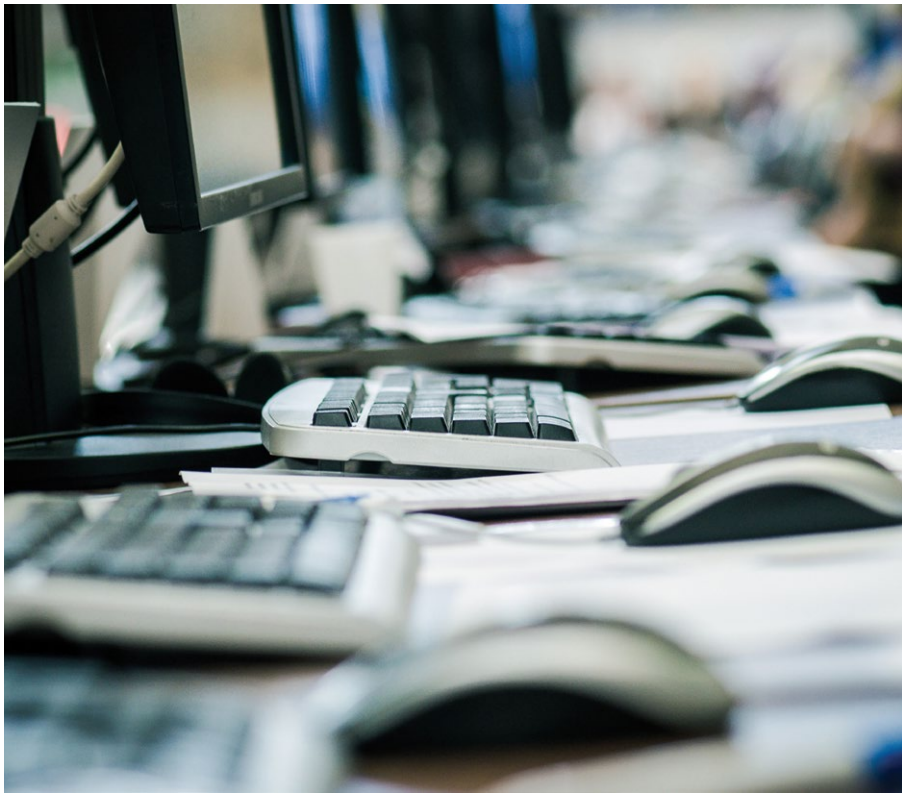


Сергей Веряскин,
генеральный директор ООО «Версия»

«В результате применения специализированных высокоскоростных плат захвата трафика наши клиенты – компании связи, в том числе сотовой, в режиме реального времени получают подробную информацию об оказанных услугах для абонентов. Они в состоянии предпринимать все новые шаги по пути оптимизации инфраструктуры и введения новых услуг для пользователей на основе глубокого анализа и в конечном счете знания потребностей клиентов и моделей использования услуг»...

Платы могут устанавливаться и работать в стандартных типовых серверах. Важной задачей адаптеров в этой связи является аппаратная предобработка, фильтрация и разделение данных с целью снижения загрузки CPU серверов. Для этого функционал позволяет равномерно распределять нагрузку на все доступные или отведенные ядра процессоров (до 128 CPU), что в среднем составляет не более 5% загрузки одного ядра.

Устанавливаемые «Версией» платы идеально подходят для высокоскоростных приложений захвата и анализа данных, с возможностью воспроизведения записанных сегментов трафика. С их помощью осуществляется сетевой мониторинг, анализ и фильтрация, а также сетевое тестирование.



Идеологической основой адаптера является технология ПЛИС (Программируемая логическая интегральная схема), которая позволяет высокоэффективно решать сложные задачи, даже на скоростях выше 100 Гбит/с. Именно единая логика позволяет безболезненно масштабировать решения в будущем и переходить на более скоростные потоки, не предпринимая фундаментальных изменений в программном обеспечении приложений.

Важной сферой применения инновационной продукции ООО «Версия» является мобильная связь, известная своим практически глобальным охватом крупных населенных пунктов, но и известной уязвимостью перед лицом кибератак. В частности, мобильному оператору необходимо оборудование для мониторинга и анализа использования сети и обслуживания в реальном времени и обработки взрывного роста трафика данных в своих сетях, а также ясного понимания, как абоненты использовали услуги передачи данных. Важно применение принципа гарантированного качества опыта (QoE) на фоне неизменного требования монетизации сетевой

Немаловажной особенностью «акселераторов» является наличие вставки высокопрецизионной (до 4 нс) аппаратной метки, присваиваемой каждому пакету, поступившему на порт адаптера. Это позволяет адаптеру объединять весь массив поступающих данных с разных портов в единый логический поток и значительно облегчить дальнейшую обработку. Наличие высокоточной аппаратной временной метки открывает путь к особо требовательным секторам, где любая погрешность или задержка оказывают прямое влияние на экономику, финансы, безопасность или эффективность работы соответствующей структуры.

инфраструктуры в соответствии со всеми новыми тенденциями.

Ясно сознавая эти требования, «Версия» помогает мобильным операторам внедрить обработку метаданных на основе глубокого анализа пакетов (DPI), что позволило компании серьезно проанализировать свой основной сетевой трафик в реальном масштабе времени на максимальных скоростях сети. Для этого использовались специальные платы-акселераторы, способные анализировать данные в GTP и IP-in-IP туннелях. Использовались карты-акселераторы с коммерческим оборудованием сервера, которое помогло сократить время развертывания и существенно снизить затраты.

Эта новая способность значительно подняла оценку клиента и лояльность и позволила мобильному телеоператору, применяющими платы от ООО «Версия» более эффективно монетизировать свои сети.

РФ

Версия

ООО «Версия» известно на телекоммуникационном рынке России с 1998 г. Компания прошла путь от дистрибьютора импортного оборудования до современного производителя и разработчика программных продуктов для телекоммуникационного рынка России.

Разработки группы компаний в области тестирования линий связи получили признание операторами связи и строительно-монтажными организациями в России и экспортируются за рубеж. Группа программистов компании с 2008 года работает над решениями контроля качества каналов связи и SLA. Программно-аппаратный комплекс wiSLA, разработанный группой компаний, является признанным стандартом в контроле качества каналов связи и управления SLA в России.

Компания активно взаимодействует более чем с 50 ведущими мировыми производителями приемо-передающего, измерительного, лабораторного и монтажного оборудования для телекоммуникаций, среди которых – ECI Telecom, EXFO, Apex T, GlimmerGlass, Napatech, Lightel, Spirent, Teraxion, Fujikura.

ООО «Версия» строит долгосрочное партнерства со своими клиентами, основываясь на инженерном опыте, инновациях и глубокой отраслевой экспертизе. Компания специализируется на ИТ-проектах в нефтегазовой, финансовой отраслях, энергетике, а также государственном и муниципальном управлении.

ПАВЕЛ ХИЛОВ:
ПРИБЛИЖАЯ ЭРУ ЭЛЕКТРОННОГО ГОСУДАРСТВА И ЦИФРОВОЙ ЭКОНОМИКИ

Гостем третьего выпуска нашей традиционной рубрики «Крупным планом» стал Павел Евгеньевич Хилов, руководитель Экспертного центра электронного государства – некоммерческой организации, занимающейся всеми аспектами внедрения информационных технологий в госуправление, а также импортозамещением в области IT.

Павел Хилов – выпускник математико-механического факультета Санкт-Петербургского государственного университета. В Высшей школе менеджмента этого же университета он прошел профессиональную переподготовку по специальности «Менеджмент». Трудится в сфере информационных технологий с 1991 года. С 2009 по 2012 год был руководителем направления региональной информатизации, а затем начальником отдела региональных программ и проектов Минкомсвязи России.

Мы беседуем с Павлом Хиловым по завершении пятого Всероссийского форума региональной информатизации «ПРОФ-IT», ежегодно организуемого Экспертным центром электронного государства. В рамках этого представительного форума прошла, в частности, ярославская премьера журнала «РАДИОФРОНТ».

Алексей ТУРБИН,
главный редактор журнала «Радиофронт»

Ольга КЛИМЕНКО

Фото: из личного архива Павла Хилова

– Павел Евгеньевич, для начала – вполне ожидаемый вопрос: чем занимается Экспертный центр электронного государства?

– Мы – российская организация, специализирующаяся на экспертизе в области формирования государственной политики по различным аспектам использования информационных технологий в органах власти. Деятельность Экспертного центра направлена на развитие и внедрение технологий электронного государства на всех уровнях власти, а также обеспечение независимого общественного контроля за этим важным процессом.

Экспертный центр объединяет более ста экспертов по ключевым направлениям развития информационно-коммуникационных технологий (по составу см. http://d-russia.ru/nashi-eksperty). В нашей работе принимают участие руководители региональных министерств и департаментов информатизации и ряда городов, ассоциации муниципалитетов, экспертное сообщество. В своей работе Экспертный центр взаимодействует с Администрацией Президента РФ, Аппаратом Правительства РФ, Минкомсвязью России, Минэкономразвития, другими федеральными органами исполнительной власти.

Следует особо отметить, что в соответствии с поручениями Президента В.В. Путина на базе Экспертного центра электронного государства, Института развития интернета (ИРИ) и Ассоциации разработчиков программного обеспечения (АРПП) «Отечественный софт» в сентябре прошлого года создан Центр компетенций по импортозамещению в сфере информационно-коммуникационных технологий (http://ru-ikt.ru/). Это автономная некоммерческая организация, деятельность которой направлена на решение практических, методических и организационных вопросов, связанных с реализацией государственной политики по импортозамещению. Среди таких вопросов – анализ проблем импортозамещения в сфере ИКТ, совершенствование законодательства в этой области, разработка методических рекомендаций по повышению эффективности работы Единого реестра ПО, функциональное тестирование продуктов и решений из Единого реестра ПО, в том числе на совместимость между собой и с аппаратным обеспечением, а также мониторинг реализации проектов по импортозамещению.

«Россия должна по определению, вне зависимости от политической конъюнктуры, внедрять свои программные продукты и «железо» – это необходимо для собственного развития, и дело тут не в ограничениях и санкциях»...

Владимир Путин,
Президент Российской Федерации

– Возглавляемый вами Центр широко известен, в частности, как учредитель информационно-аналитического портала D-Russia.ru. В чем его особенности?

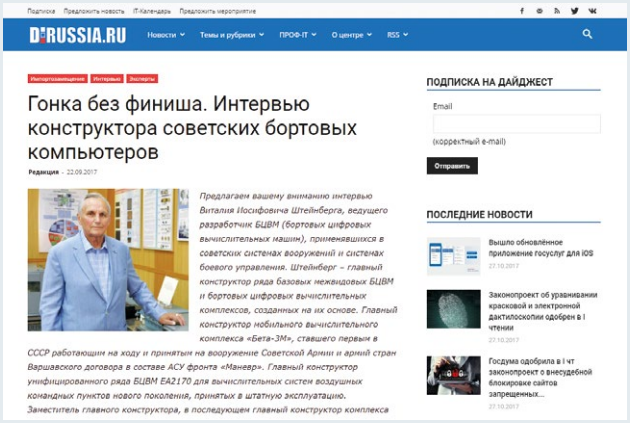
D:RUSSIA.RU

– «Цифровая Россия» (Digital Russia) – это фактически единственное в нашей стране ежедневное информационно-аналитическое издание, целиком и полностью посвященное вопросам государственной информатизации. Оно специализируется на новостях и аналитических материалах по таким темам, как передовой отечественный и зарубежный опыт применения IT в государственном управлении, цифровая экономика, электронное правительство, государственная политика, место России в современном IT-мире, управление интернетом и многое другое.

Особое внимание D-Russia уделяет импортозамещению в области программного обеспечения, нормативному регулированию в сфере ИКТ, лучшим практикам использования IT в различных областях государственного управления.

Экспертный центр объединяет более ста экспертов по ключевым направлениям развития информационно-коммуникационных технологий (по составу см. http://d-russia.ru/nashi-eksperty). В нашей работе принимают участие руководители региональных министерств и департаментов информатизации и ряда городов, ассоциации муниципалитетов, экспертное сообщество. В своей работе Экспертный центр взаимодействует с Администрацией Президента РФ, Аппаратом Правительства РФ, Минкомсвязью России, Минэкономразвития, другими федеральными органами исполнительной власти.

Начиная с прошлого номера, журнал «РАДИОФРОНТ» печатает избранные материалы, представленные порталом D-Russia. В свою очередь, D-Russia публикует некоторые материалы нашего журнала.



Повторюсь: наш портал не только оперативно публикует новости по этому актуальному кругу вопросов, но и предоставляет возможность представителям региональных органов власти, местного самоуправления, компаний-разработчиков ПО и других организаций высказать экспертное мнение о процессах государственной информатизации и рассказывать о лучших практиках региональной и муниципальной информатизации. Среди авторов D-Russia.ru – известные в стране IT-эксперты, руководители федеральных органов власти и представители органов местного самоуправления.

Что еще важно: помимо традиционных принципов журналистики (у нас работают отличные профессионалы с богатым опытом в сфере информационных технологий), основной наш подход в освещении событий – это достоверность. Мы не пишем о слухах и предположениях, о черновиках каких-то документов, у нас не бывает «источников, близких к …». Если мы публикуем материал, то наш читатель всегда уверен, что событие точно произошло, документ – точно принят или его проект официально опубликован, а

Игорь Щеголев,
помощник Президента Российской Федерации,
из выступления на пленарной дискуссии форума «ПРОФ-IT», 19 сентября 2017 года, Ярославль

«За последний год в стране принято несколько важных документов, которые определяют развитие ИТ-отрасли на много лет вперед: это Стратегия информационного общества до 2030 года и Программа развития цифровой экономики. Развитие цифровых технологий становится приоритетом для страны.
Масштаб «большой цифры» поднимает, помимо прочего, нравственные и этические проблемы: невозможно машине запрограммировать духовное и нравственное начало.
Регионам необходимо обновить социальные лифты, чтобы молодые люди применяли свои знания на местах, а не только в Москве или за границей.
У нас нет задачи гнаться за так называемыми прорывными технологиями, многие из которых впоследствии оказываются мифами. Необходимо соблюдать принцип разумной достаточности применения технологий и сбора данных. Стратегия информационного общества требует найти баланс между технологиями и интересами граждан».

«Цифровая Россия» (Digital Russia) – это фактически единственное в нашей стране ежедневное информационно-аналитическое издание, целиком и полностью посвященное вопросам государственной информатизации. Оно специализируется на новостях и аналитических материалах по таким темам, как передовой отечественный и зарубежный опыт применения IT в государственном управлении, цифровая экономика, электронное правительство, государственная политика, место России в современном IT-мире, управление интернетом и многое другое. Особое внимание D-Russia уделяет импортозамещению в области программного обеспечения, нормативному регулированию в сфере ИКТ, лучшим практикам использования IT в различных областях государственного управления.

назначение – точно состоялось. И поскольку около половины наших постоянных читателей составляют представители органов власти всех уровней, то этот подход вполне оправдан, так как зачастую именно наш ресурс является для них первоисточником той или иной информации.

– Одной из важных событийных тем, широко освещенных на D-Russia.ru в последнее время, стал очередной Всероссийский форум региональной информатизации «ПРОФ-IT». Несколько слов о нем, пожалуйста...

– Он очередной, но не обычный, а юбилейный, пятый по счету. Форум прошел 19-20 сентября в Ярославле и закрепил, как нам представляется, свою репутацию ведущей IT-площадки в области государственного управления. По количеству участников и представленных регионов форум стал рекордным: в этом году к нам приехали около 300 делегатов из 53 регионов страны, при этом от большинства регионов были руководители органов власти, ответственных за информатизацию.

Форум состоит из двух больших блоков – это пленарное заседание и тематические секции, с одной стороны, и с другой – финальная часть Всероссийского конкурса проектов региональной и муниципальной информатизации «ПРОФ-IT». Темы для обсуждения в дискуссионной части определяются в результате опроса основных

участников – региональных IT-руководителей. Так, в этом году разговор шел о новой стратегии развития информационного общества, программе «Цифровая экономика Российской Федерации», информационной безопасности, в том числе в применении к модным ныне «прорывным» технологиям, об импортозамещении в сфере ИКТ, об оптимизации и автоматизации контрольно-надзорной деятельности государства, об образовании в сфере ИТ и о другом.

– В чем суть конкурса? Кто в нем соревнуется и зачем это участникам?

– С 2013 года конкурс проводится среди региональных органов власти, которые представляют на суд своих коллег разработанные и, что важно, внедренные информационные системы по нескольким номинациям (ИТ в здравоохранении, образовании, социальной защите, безопасности, управлении транспортом и т.п. – всего их 14). Он проходит в два этапа – заочная оценка региональным жюри, в результате которой отбираются финалисты, и очная защита проектов.

С 2013 года конкурс проводится среди региональных органов власти, которые представляют на суд своих коллег разработанные и, что важно, внедренные информационные системы по нескольким номинациям (ИТ в здравоохранении, образовании, социальной защите, безопасности, управлении транспортом и т.п. – всего их 14). Он проходит в два этапа – заочная оценка региональным жюри, в результате которой отбираются финалисты, и очная защита проектов.

Так, в этом году на конкурс было принято 103 проекта, 43 из которых вышли в финал и принимали участие в очной защите в Ярославле. По результатам защиты в числе лидеров по количеству наград в этом году – Ханты-Мансийский автономный округ – Югра и Санкт-Петербург. Также необходимо отметить, что пока единственным регионом, который собрал всю коллекцию статуэток «ПРОФ-IT», является Свердловская область, уверенно удерживающая уже пять лет первую позицию в номинации «IT в социальной сфере».

Отдельно хочу отметить, что конкурс проводится без какого-то административного ресурса, региональных руководителей привлекают две возможности, которые он дает: показать свои наработки коллегам из других регионов и заработать награду, если работа ее заслужит, и получить полную картину того, что происходит в региональной информатизации в целом.

– Вы уже неоднократно упомянули проблематику импортозамещения. Нашел ли выражение ее региональный аспект на ярославском форуме «ПРОФ-ИТ»?

– Экспертный центр электронного государства уже несколько лет работает над «продвижением» темы импортозамещения и на федеральном, и на региональном уровнях. Еще в 2015 году на «ПРОФ-IT», который прошел в Ханты-Мансийске, мы провели первую секцию по обсуждению проблематики импортозамещения в органах власти, которая выявила достаточно много острых вопросов и проблем. После этого нами (и не только нами, конечно) было организовано еще множество мероприятий на эту тему. В 2015-2016 годах был принят ряд концептуальных документов, нормативно закрепивших курс на ИТ-независимость государства от зарубежного программного и аппаратного обеспечения.

Мы уже второй год в число номинаций конкурса включаем номинацию «Лучший проект по импортозамещению» и получаем достаточно много интересных конкретных решений, которые показывают, что процесс «пошел». Уже можно говорить о реальных достижениях и о системной работе, которая ведется в некоторых регионах.

На страницах D-Russia.ru мы стараемся подробно и содержательно писать о таком опыте коллег, отмечая и их достижения, и проблемы, с которыми они сталкиваются. Для этого есть специальная рубрика – «Импортозамещение», в которой, кстати, недавно были опубликованы несколько интересных материалов – об опыте Челябинской и Тульской областей, о методологии перехода на российское ПО.

Отдельно можно сказать, что «ПРОФ-IT» интересен и для российских компаний – разработчиков программного обеспечения и телеком-оборудования. Партнерство бизнеса с площадкой «ПРОФ-IT» позволяет налаживать тесный контакт с потенциальными клиентами и продвигать отечественные компании на рынке региональной информатизации и, напротив, информировать региональных IT-руководителей об интересных решениях, разработанных нашими компаниями.

– Павел Евгеньевич, каковы ближайшие и стратегические планы возглавляемого вами Экспертного центра электронного государства?

– Если говорить о развитии «форумного» и «конкурсного» направлений, то мы сейчас прорабатываем несколько новых форматов, которые призваны сделать более эффективными «горизонтальное» общение на региональном и на муниципальном уровнях. Есть много других идей, о которых преждевременно говорить, пока мы не приступим к их реализации.

Важное направление – развитие ресурса D-Russia.ru, мы хотим сделать его действительно основным источником информации об использовании ИТ в государственном управлении. Совсем недавно мы радикально изменили внешний вид и функционал нашего сайта, и теперь дело только за реализацией всех возможностей, которые у нас появились в результате «переезда». Здесь тоже много направлений, которые мы последовательно планируем развивать, включая и дополнительные сервисы для посетителей, и новые форматы подачи информации, и расширение партнерства с интересными изданиями, и более активное сотрудничество с регионами.

Кстати, хочу отметить, что с 2014 года мы не рассматриваем предложения о партнерстве со стороны зарубежных производителей «железа» и ПО, хотя предложений получаем по-прежнему много, и это принципиальная позиция.

Второе важное направление – это развитие ресурса D-Russia.ru, мы хотим сделать его действительно основным источником информации об использовании ИТ в государственном управлении. Совсем недавно мы радикально изменили внешний вид и функционал нашего сайта, и теперь дело только за реализацией всех возможностей, которые у нас появились в результате «переезда». Здесь тоже много направлений, которые мы последовательно планируем развивать, включая и дополнительные сервисы для посетителей, и новые форматы подачи информации, и расширение партнерства с интересными изданиями, и более активное сотрудничество с регионами.

– Спасибо вам за эту беседу.

РФ

Этапы плана импортозамещения ПО в Челябинской области:

I этап (до конца 2018 года): переход на использование отечественного прикладного программного обеспечения с сохранением на компьютерах существующей операционной системы. Тестирование комплексного решения по импортозамещению IT-инфраструктуры в органах местного самоуправления.

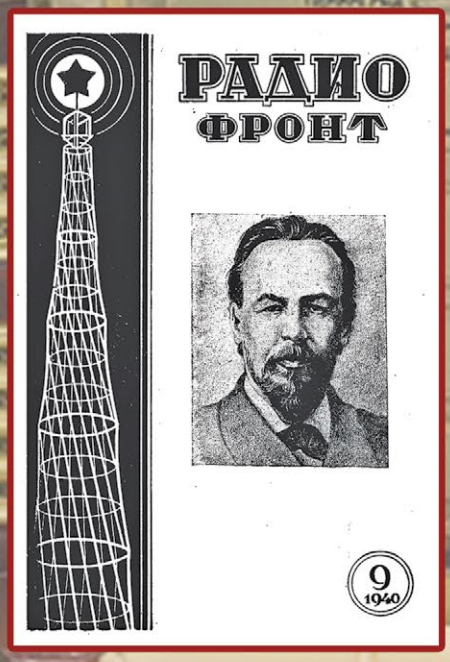
II этап (до конца 2019 года) – формирование инфраструктуры переходного периода, установка внутри отечественной операционной системы виртуализации, позволяющей запускать привычную пользователям среду Windows;

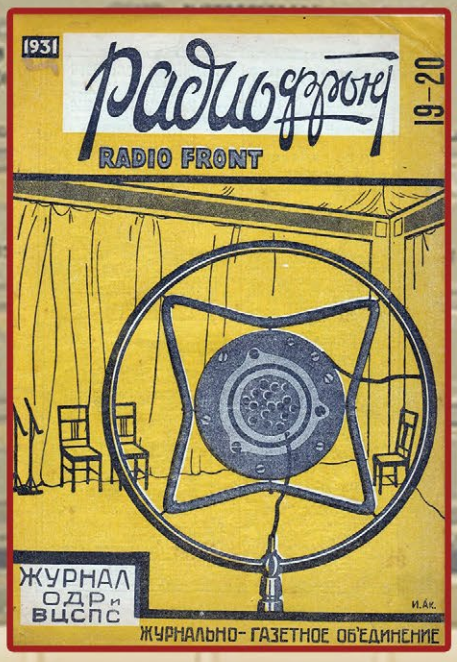
III этап (2020 год) – полное завершение перехода Челябинской области на использование отечественного программного обеспечения.

журнал

Радиофронт

Исторический ракурс





В этом выпуске «Исторического ракурса» мы представляем материалы из журнала «Радиофронт» 1931 года, которые связаны общей темой – военного применения радиодостижений, борьбой с классовыми врагами, повышением пролетарской бдительности в рядах профессионалов и любителей тогда еще совсем нового, но уже весьма массового внедрения радиодостижений в самые разные сферы жизни. Правописание и пунктуация сохранены!

ИЗОБРЕТАТЕЛЬСТВО — ФРОНТ КЛАССОВОЙ БОРЬБЫ

Иные полагают, что радио в наших условиях – лишь только орудие повышения нашей культурности. Иные, чувствуя, что надо дать политическую оценку значению радио у нас, добавляют – орудие культурной революции. А третьи, зная, что вышеуказанные односторонние оценки являются грубейшей политической ошибкой, граничащей с вредительством, недостаточно энергично боролись, не давали отпора и не искореняли такие представления, оставляя дело радио в руках «аполитичного» и оппортунистического руководства.

Советское радио не только пропагандист, агитатор и организатор нового быта. Оно – острейшее и гибчайшее орудие классовой борьбы в руках пролетариата. Радио борется за промфинплан па предприятии, дает бой кулаку, организуя колхозные поля, оно повседневно, повсенощно и ежечасно бьется за генеральную линию партии.

Вредители не оставили без внимания эту отрасль нашего строительства. Они успела кое в чем напортить технически: хаос в эфире. Мы имеем также политические прорывы на фронте радиовещания. Но хуже дело обстоит с организацией радиослушателя, потому что руководство направлением работы советских радиолюбителей в течение ряда лет оставалось в руках аполитичных специалистов.

Наша радиопресса культивировала делячество (дело – ради дела) в среде радиолюбителей, прививала филистерский индивидуализм радиолюбительской массе. Радиолюбители бились за «дальнобойность» своего (!) приемника не для того, чтобы, скажем, сибирский колхозник или уральский рабочий слушал «Коминтерн», а ради того, чтобы, слушая «нежное банджо» «экзотической» Явы или сногсшибательный шимми «веселого и беспечного» Будапешта (кто сравнивал число фокстротирующих с числом безработных в «веселом и беспечном» Будапеште?), отстроиться от политики, которой так боится «аполитичный» спец и которую так не любит обыватель, особенно в своем царстве мещанского уюта, где он прячется от коллектива и треволнений нашей эпохи.

Именно ради такой «дальнобойности» «боролись с Москвой»..., извиняюсь, боролись за избирательность своего приемника.

Коротковолновики наши занимались рекордсменством и лишь от случая к случаю связывались с Красной армией или с научными экспедициями.

Наше радиолюбительство не было проникнуто боевым духом большевистской партийности. Оно было насквозь пропитано делячеством, культивировало в своей среде ограниченность и убожество мещанской философии и вкуса, скатываясь в болото аполитичности.

Все эти настроения нашли свое отражение в развитии нашей радиотехнической промышленности. Здесь с чрезвычайной отчетливостью проявился закон обратного влияния надстройки на базис, выведенный марксовой диалектикой. Оппортунистическая установка на индивидуальную радиоточку выразилась в выпуске дешевого «массового» детекторного приемника (ЛД) (равнение на узкие места) и знаменитого БЧ на «микрушках», который никак не хочет еще ложиться в гроб вслед за своей партнершей. Промышленность занималась индивидуальными приемниками, а трансляционные узлы самотеком и кустарно, черепашьими темпами росли как самосейка.

Еще более своеобразно протекала борьба за совершенную советскую радиолампу. Вредители очень искусно поддерживали в промышленных

кругах мнение, что нам, мол, незачем ориентировать свою продукцию на капризные запросы и претензии квалифицированного любителя, профессионала и рекордсмена. Мы, мол, для рабочих, для деревни...

Оппортунисты отказывались хоронить «микрушку», лопоча что-то о своеобразии путей нашего развития. Электрификация, мол, не поспеет развить нужные темпы и дать энергию деревне. Куда нам до подогревных, экранированных, оксидных! Мы ужо на «микрушках» да на батарейках будем перегонять (т.е. и здесь имело место отражение оппортунистической установки на индивидуальную точку).

Расчеты и чаяния вредителей опрокинуты. Оппортунистическое словоблудие разбито самой жизнью.

Мы имеем лампы с оксидными катодами, подогревные, экранированные. «Светлана» выполнила наперекор всем маловерам и нытикам пятилетку в 2,5 года. «Микрушка» положена в гроб – осталось заколотить гвозди. Поредовики-«светлановцы» награждены орденами Красного трудового знамени.

Но борьба еще не закончена.

Еще нет на рынке советского пентода, может быть мало интересного

УСКОРИТЬ ПЕРЕСТРОЙКУ ПОЛИТИЧЕСКОГО РАДИОВЕЩАНИЯ
РЕШИТЕЛЬНЕЕ РАЗОБЛАЧАТЬ СОПРОТИВЛЕНЦЕВ И «ЛЕВЫХ» ФРАЗЕРОВ

любителю индивидуалу, но необходимого колхозным трансляционным узлам и мощным узлам рабочих городов строящихся промышленных гигантов.

Еще нет электродинамического громкоговорителя, нет совершенного, стандартного приемника, нет измерительных приборов для обслуживания установок с дорогими лампами, для ведения технически грамотного режима их.

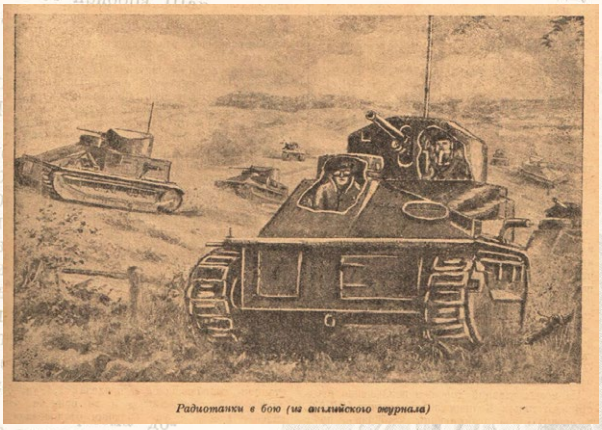
Нет приборов, подчеркиваем, для экспериментаторских, исследовательских работ в лабораториях, и научно-исследовательских институтах, которые разрослись (количественно и по охвату ими количества и качества решающих проблем) и теперь буквально задыхаются от недостатка аппаратуры.

Это дело (приборостроение) должно быть решительно двинуто вперед, ибо «экономия подчас бывает худшею растратой» (Безыменский) нашего времени, наших темпов, качества нашей работы.

Радиопромышленность еще не совершила скачка, неизбежность которого обусловлена общественным развитием – решающими победами на фронте индустриализации и технико-экономической революцией в нашем сельском хозяйстве, происходящей на основе сплошной коллективизации и ликвидации кулачества как класса.

Помехи радиостанций противника

Чтобы мешать работе радиосвязи станции противника, мешающая сторона должна располагать прежде всего более мощными радиостанциями, располагаемыми на близком расстоянии от тех радиостанций, работе которых нужно помешать. Эта возможность на поле боя весьма проблематична, так как большую трудность представит укрытие антенн и аппаратов. Таким образом, если применять для мешания мощные радиостанции, то их приходится располагать вдалеке от фронта; если же применять для этого маломощные передатчики, то эффект их воздействия будет незначителен. Но даже при предположении, что противнику удастся расположить достаточно мощные мешающие передатчики и достаточно близко к фронту, то и в этом случае, при применении радиостанций, работающих незатухающими колебаниями, и приемников с большой избирательностью, достаточно минимальное изменение длины волны работающих радиостанций, чтобы иметь возможность вести работу без ощутительного влияния помех от мешающих передатчиков.



Радиотанки в бою (из английского журнала)

Применение подобных незначительных, едва заметных изменений длины волны рекомендуется и при обычной работе радиостанций, чтобы этим с одной стороны, уменьшить возможность подслушивания, а с другой стороны, избежать возможности мешания.

Отрицается также действительность производства мешающих воздействий при помощи старых искровых радиостанций, так как затухающие волны, комбинируясь с местными колебаниями приемных станций, теряют свою тональность и производят в телефоне звуки, настолько отличающиеся от чистого звука, производимого незатухающими колебаниями, что для опытного слухача не представит трудности выделить нужные сигналы из помех.

Наконец, следует учитывать то обстоятельство, что, если радиостанция противника работает на создание помех, то она мешает и работе своих подслушивающих станций, в то время как разведывательные радиостанции другой стороны не лишаются возможности вести свою работу.

Указанные соображения делают возможность широкого использования мешания маловероятным. Легче всего мешать работе радиостанций, установленных на самолетах, корректирующих артиллерийский огонь и часто находящихся на более далеком расстоянии от корреспондирующих с ими радиостанций, чем мешающие радиостанции.

Рассмотрев все основные вопросы, возникающие при использовании радио на поле боя, можно резюмировать все выводы следующим образом:

1) Возможность поддержания связи, представляемая радио, имеет настолько большое всей военное значение, что применение его в наиболее трудные моменты боя, когда никакое другое средство связи не может его заменить, абсолютно необходимо.

2) Современные радиотелеграфные приборы делают возможным и выгодным использование радио для связи не только крупных войсковых соединений, но также и в передовой полосе.

3) Важнейшими недостатками радиосвязи являются медленность и возможность подслушивания.

4) Правила использования радиотелеграфа можно свести к следующим:

а) радиостанции при широком их применении должны в полной мере использовать избирательность современных приемных устройств;

б) при использовании радиостанций всегда нужно пользоваться исключительно шифром;

в) при организации радиосвязи всегда следует проявлять заботу о срочности и секретности передаваемого. При этом в крупных войсковых соединениях наибольшее внимание следует обращать на секретность передаваемого, а в небольших соединениях – на достижение быстроты связи;

г) радиосвязь в небольших войсковых соединениях должна быть особенно приспособлена к передаче коротких и срочных сообщений.

д) радио, как правило, не должно совершенно применяться во время периодов затишья и подготовки к операциям;

е) радио было и остается средством связи во время наиболее острых, динамичных и решающих моментов войны и боя.

Передача изображений на расстояние

В разрешении проблемы передачи изображений па расстояние, впервые

поднятой уже несколько десятков лет назад, только в последние годы наметились определенные успехи, сулящие возможность ее полного практического осуществления. Значение ее настолько велико как для гражданской жизни, так и для военного дела, что нет ни одного государства с крупно развитой техникой, которое в более или менее широком масштабе не вело бы работ для ее разрешения.

О военном использования приборов для передачи изображений на расстояние известно следующее. Военные ведомства всех крупных государств с большим вниманием следят за производящимися работами, и, после принятия приборов ведомством почты и телеграфа, несомненно, примут их в качестве средства связи между крупными штабами. Прежде всего, надо полагать, передача изображений будет использована морскими ведомствами для приема метеорологических бюллетеней на судах.

«Дальновидение»

Во многих государствах, помимо опытов по передаче изображений от пункта к пункту, производятся испытания по передаче кроков и несложных набросков с самолета. В Германии фирмами Телефункен и Лоренц разработаны отличающиеся большой портативностью приборы передачи изображений для обслуживания нужд полиции.

Игнорирование рабочего шефства

Завод «Мосэлектрик» шефствует над Наркомпочтелем. Рабочие завода послали в радиоуправление специальную бригаду для проверки выполнения предложений комиссии по чистке. Казалось бы, общественность радиоуправления обязана была оказать бригаде всяческое содействие и помощь.

Что же получилось на деле?

Секретарь (бывший) ячейки т. Степной вместо поддержки бригады начал всячески ее игнорировать.

«С материалами чистки я недостаточно знаком, – заявил он бригаде. – Притом вы же не туда попали. Не дело партийной ячейки заниматься такими делами. По этому вопросу необходимо обращаться в местком».

Оппортунистический чиновник не мог попять самой простой вещи – партийная организация не только должна знать решения комиссии по чистке, но и отвечать за их выполнение.

Впрочем, такое отношение к рабочему шефству оказывается не случайно: оно обосновано даже «теоретическими» установками т. Смирнова, который считает, что рабочее шефство – это «вмешательство в руководство радиовещанием, что является совершенно неправильным с точки зрения основной установки партийного руководства радиовещанием».

Неправильность такой «теории» совершенно очевидна. Тов. Смирнов боится рабочего шефства. Он не хочет, чтобы рабочие контролировали его работу.

Рабочая бригада имеет полное право вмешиваться в руководство радиовещанием, если на этом участке искривляется линия партии, процветает самый махровый оппортунизм. А что это на самом деле так, об этом ясно и четко сказано в решениях Краснопресненского райкома партии.

«Активный» баланс радиовещания

Что сказал райком о состоянии политического радиовещания?

Отметив, что «бюро ячейки прошло мимо ряда крупнейших прорывов, не перестроившись лицом к своему производству, и не мобилизовало массы па преодоление узких мест, допустив этим ряд политических ошибок, являющихся по своему характеру правооппортунистическими», райком констатировал:

«Наличие правооппортунистических искривлений в практике руководства политвещанием («немассовость», «беззубость», оппортунистические вывихи – см. «Правда» от 25 марта, 7 апреля и 4 июля).

Наличие правооппортунистических извращений в практике художественного радиовещания (использование на исследовательской работе чуждых элементов, полная изолированность от музыкальной пролетарской общественности, отсутствие отпора и разоблачений со стороны партруководства реакционным буржуазным установкам в вопросах искусства Лапицкого («Искусство – товар», «Работа на потребителя» и т. д.).

Наряду с этим райком отметил также «недостаточное и запоздалое реагирование на обзоры «Правды» со стороны ячейки, осужденные в последующих обзорах «Правды», и полное игнорирование со стороны партруководства РУ и бюро ячейки сигналов других органов печати (журналы: «Рост», «Радиофронт», «За пролетарскую музыку», газеты: «За компросвещение», «Радио в деревне», «Труд», «Литературная газета»).

Таковы «скромные» итоги политического радиовещания.

Решения Краснопресненского райкома партии дают четкие и ясные определения положению на радиофронте.

Мы уже неоднократно сигнализировали о тревожном положении в эфире.

Райком отстранил оппортунистов от партийного руководства. Контрольная комиссия вынесла всему составу бюро выговор.

Решение Краснопресненского райкома партии должно быть началом решительного изгнания всех оппортунистов из радиоуправления, тормозящих коренную и решительную перестройку этого ответственного участка.

Надо, наконец, по-большевистски взяться за перестройку политического радиовещания.

Вопрос о перестройке политического радиовещания – принципиальный вопрос. И мы должны твердо помнить, что без решительной борьбы с оппортунизмом, «левым» фразерством, примиренчеством, нельзя осуществить перестройку политического радиовещания, нельзя его большевизировать.

РАЗВИТИЕ НАЦИОНАЛЬНОЙ ЭЛЕКТРОННОЙ КОМПОНЕНТНОЙ БАЗЫ

В начале ноября в Москве в помещении АО «Рособоронэкспорт» состоялось заседание Координационного совета разработчиков и производителей радиоэлектронной аппаратуры, электронной компонентной базы (ЭКБ) и продукции машиностроения Союза машиностроителей России и секции № 4 МРГ по ЭКБ при коллегии Военно-промышленной комиссии Российской Федерации.

Основной темой дискуссии стало правоприменение законодательства об ограничениях и запретах допуска радиоэлектронной продукции, происходящей из иностранных государств, к закупкам для обеспечения государственных и муниципальных нужд, а также о преференциях предприятиям, производящим радиоэлектронную продукцию российского происхождения, при осуществлении закупок компаний с государственным участием, предусмотренных Постановлением Правительства РФ от 17.07.2015 № 719 «О критериях отнесения промышленной продукции к промышленной продукции, не имеющей аналогов, произведенных в Российской Федерации».

Председатель Координационного совета разработчиков и производителей радиоэлектронной аппаратуры, электронной компонентной базы и продукции машиностроения, заместитель генерального директора – статс-секретарь АО «Росэлектроника» Арсений Брыкин во вступительном слове подчеркнул, что нынешняя повестка связана с вопросами импортозамещения: «Нужно понимать, что без радиоэлектроники и цифровой экономики импортонезависимость недостижима. Основная задача Координационного совета – разработать предложения, которые помогут в решении данных вопросов. Также необходимо подвести итоги полугодовой деятельности рабочей группы нормативно-правового регулирования отрасли при Координационном совете».

Обсуждение подобных тем проходило в рамках подготовки к заседанию Экспертного совета Госдумы по радиоэлектронике. «Мы пришли к пониманию важности правильных формулировок в нормативно-правовом поле. Тем не менее критерии отнесения продукции к произведенной в России не требуют наличия у физических лиц прав на технологическую документацию и исходные коды программного обеспечения. Действующие ограничения и запреты иностранной продукции не распространяются на закупки компаний с государственным участием. Ну и 15-процентная преференция для отечественных производителей в том числе малого и среднего бизнеса не способствует увеличению спроса на отечественную радиоэлектронную продукцию в рамках закупок компаний в том числе с государственным участием. Поэтому в законодательство необходимо внести изменения», – подчеркнул Арсений Брыкин.

Академик РАН, научный руководитель Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» Владимир Бетелин выразил мнение, что сила IT-отрасли не в гигабайтах и нанометрах, а в экономике. В том, какие товарные обороты эта отрасль имеет: «Цифровая экономика – это программа, которая уже полностью оформлена. Мы живем в цифровой эре. За тем же блокчейном стоят огромные полупроводниковые обороты. На сегодняшний день смартфоны есть у 60% населения. Это положительный факт, но в прошлом году куплено 30 млн смартфонов именно зарубежных производителей. На этом примере видна критическая зависимость России от импорта. В других отраслях также наблюдается подобная ситуация. Если мы будем двигаться по подобному пути, то нам так и придется в дальнейшем зависеть от зарубежных производителей. Именно внутренний рынок является первой ступенью для будущего роста цифровой экономики. Проблема импортозамещения – это проблема отсутствия в России социально-экономической области. Поэтому сейчас Россия многое вынуждена покупать за рубежом».

Руководитель рабочей группы по нормативному регулированию отрасли Координационного совета, руководитель Управления взаимодействия с органами государственной власти АО «Росэлектроника» Татьяна Львова озвучила предложения по внесению изменений в нормативно-правовые акты: «Для того, чтобы меры защиты внутреннего рынка заработали, необходимо решить проблему, которая связана с отсутствием в законодательстве на уровне федерального закона критериев высокотехнологичной продукции российского происхождения. Таких критериев на сегодняшний день нет. В итоге это приводит к тому, что в 719-м постановлении, которое, по сути, является постановлением рамочным, отсутствует такое требование, как наличие у российского юридического лица прав на интеллектуальную собственность, на программное обеспечение, на конструкторскую документацию. Следствием этой проблемы является то, что российские компании не имеют возможности самостоятельно модернизировать и развивать технологии. В итоге не осуществляется технологическая и экономическая безопасность страны».

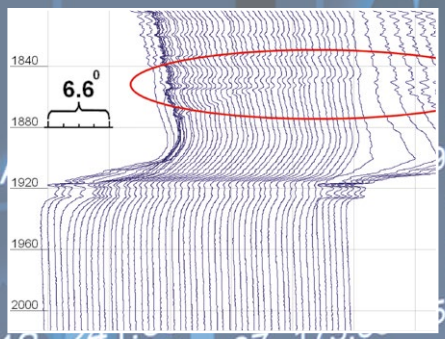
РФ

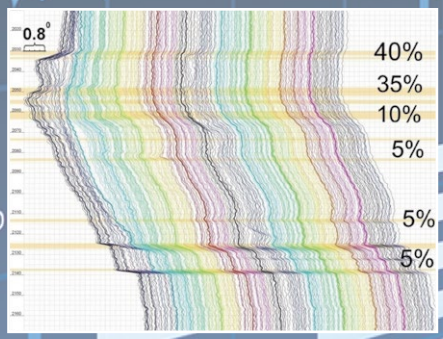
№03 (216), НОЯБРЬ 2017

НАУКА • ТЕХНИКА • ИННОВАЦИИ

РАДИОФРОНТ

НАУЧНЫЕ ПУБЛИКАЦИИ





Оптоволоконные измерения температуры в скважинах

Опыт, проблемы, перспективы

Fiber-optic temperature measurement in wells

Experience, problems and prospects

И.А. Черных
ООО «ЛУКОЙЛ-ПЕРМЬ»
I.A. Chernyh
LUKOIL-PERM

В.Ф. Рыбка
ООО «ПИТЦ «Геофизика»
V. F. Rybka
PITC Geofizika

Ю.В. Лапшина
ООО «ПИТЦ «Геофизика»
Y.V. Lapshina
PITC Geofizika

Е.А. Гринин
технический директор
группы компаний «Сертал»
E.A. Grinin
SERTAL Group Technical Director

КЛЮЧЕВЫЕ СЛОВА: оптоволокно, термометрия, контроль за разработкой, профиль притока, контроль работы скважины.

АННОТАЦИЯ: В статье кратко описан опыт работ с оптоволоконными системами измерения температуры (ОВСт) в ООО «ПИТЦ «Геофизика». Проведено сравнение технологии ОВСт с аналогами, имеющимися на сегодняшний день, и рассмотрены проблемы ее внедрения.
Имеющаяся технология уже сейчас позволяет решать задачи определения профиля притока и контроля работы скважины. ОВСт может определять процентное соотношение дебита пластов, водо-нефтяного раздела в стволе скважины и интервалы поступления воды при соблюдении определенных условий. Ее дальнейшая модификация с добавлением режима СТД и барометрии позволит решать эти задачи однозначно. Область действия ОВСт – мониторинг работы скважин. Назначение технологии в первую очередь – это управление работой месторождения.
Системы интеллектуальных скважин и интеллектуальных месторождений рано или поздно займут лидирующее положение в нефтегазодобыче. Без этих систем невозможна дальнейшая оптимизация добычи. Для того чтобы занять этот рынок услуг, необходима работа с дальнейшим продвижением ОВСт. Компания ООО «ПИТЦ «Геофизика» уже сейчас готова предложить сотрудничество в работе с данной технологией.

KEYWORDS: fiber-optics, thermometry, development control, control of development, inflow profile, control of wells.

ABSTRACT: The article briefly describes the experience of working with fiber optic temperature measurement systems in the company PITC Geofizika. It is compared of technology the fiber-optic temperature measurement systems with similar technologies available today, and are considered the problems of its implementation.
Available technology allows us to solve the problem of determining the inflow profile and control of the well now. The fiber-optic temperature measurement systems can determine the percentage of debit recovery, oil-water section of the wellbore and intervals of water flow under certain conditions. It further modification with the addition of termokonduktivnaya flowmetry (СТД) mode and barometer will allow to solve these problems clearly. The scope of the fiber-optic temperature measurement systems is monitoring of wells. The first purpose of the technology is the management of the field.
Systems intelligent well and intelligent field will take a leading position in oil and gas production sooner or later. None of these systems cannot be further optimization of production. In order to occupy the market of services necessary to work with the further advancement of fiber-optic temperature measurement systems. The company PITC Geofizika now is ready to offer cooperation in the work with this technology.

Предыстория

ООО «ПИТЦ «Геофизика», начиная с 2012 года, развивает и внедряет в производство оптоволоконные системы измерения температуры (ОВСт) по стволу скважины. На сегодняшний день это замеры в более чем 30 скважинах. [1] Получен положительный результат, и настало время подвести промежуточный итог.

Опыт, технологии

Рассмотрим в этой главе те области применения, в которых ОВСт однозначно превосходят другие способы измерения. Сравнение с имеющимися технологиями проведем ниже.

1. ОВСт однозначно решает задачи определения уровня жидкости в стволе скважины при механизированном способе добычи (рис. 1-3). Проверено на 3 скважинах с ЭЦН и на 2 с ШГН. При этом уровень определяется при работе насоса и его остановках не более чем за сутки. Определяется именно уровень жидкости, а не верх пены, как эхолотами.

Контроль уровня легко автоматизировать и затем получить автоматическое управление эффективностью добычи. Работа скважины с минимальным уровнем в большинстве случаев позволяет получить максимальный дебит.

Кроме того, имеется возможность контроля температуры насоса. При понижении уровня и нагреве насоса (рис. 1) насос должен быть автоматически переведен на меньшую производительность.

2. ОВСт определяет водо-нефтяной раздел в стволе скважины и интервалы поступления воды (рис. 4, 5) при соблюдении определенных условий работы скважины и наличии в продукции нефти. Это позволяет определить источники обводнения при смене скважинной продукции и изменить негативное развитие ситуации, управляя системой ППД. Процесс может быть автоматизирован контролем состава и дебита жидкости на устье и «ручным» принятием решения при выходе контролируемых параметров за заданные пределы по данным ОВСт.

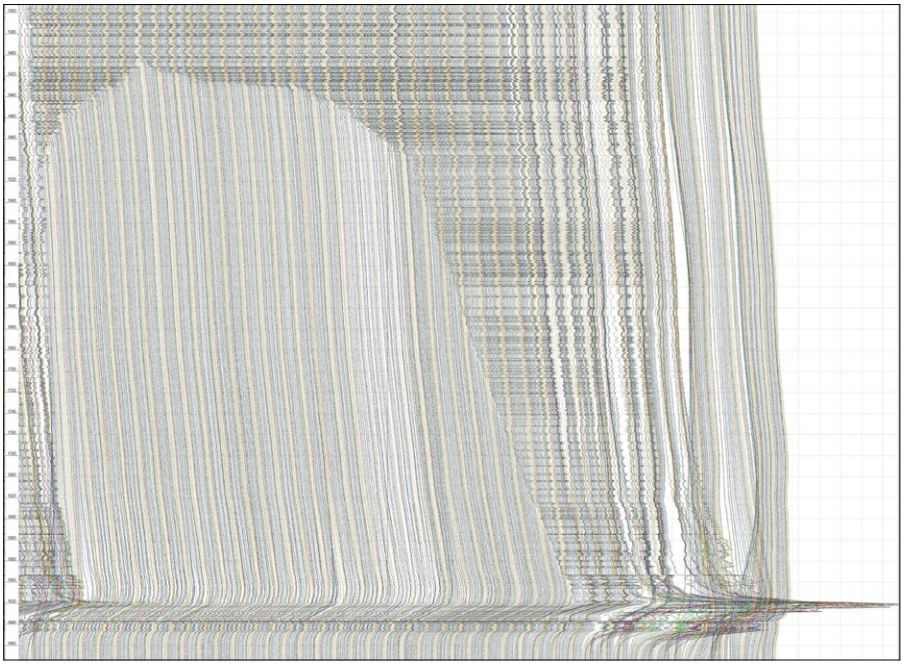


Рис. 1. **Динамический уровень при работе ЭЦН на 45 Гц, снижение уровня при переходе на 50 Гц.**

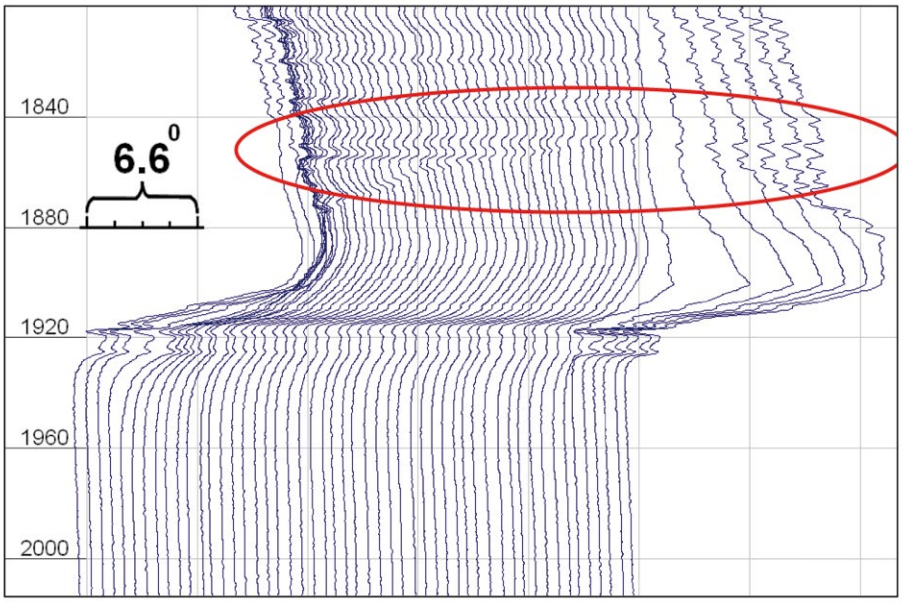


Рис. 2. **Динамический уровень при остановке и запуске ЭЦН**

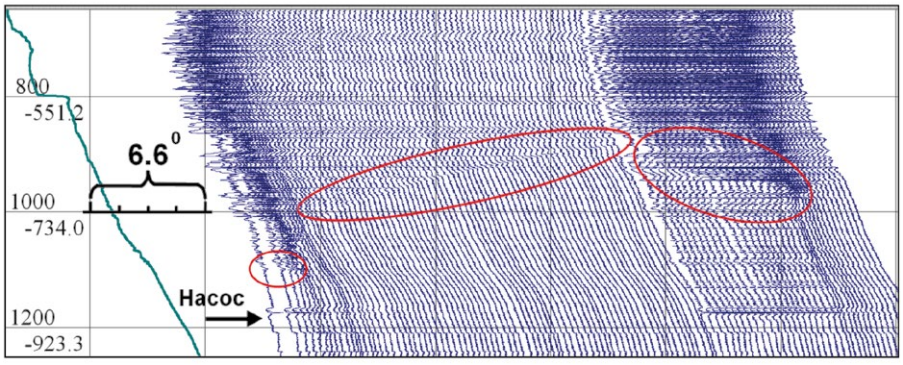


Рис. 3. **Динамический уровень при работе и остановке ШГН**

Рис. 4. **Работа пластов водой при остановке ЭЦН**

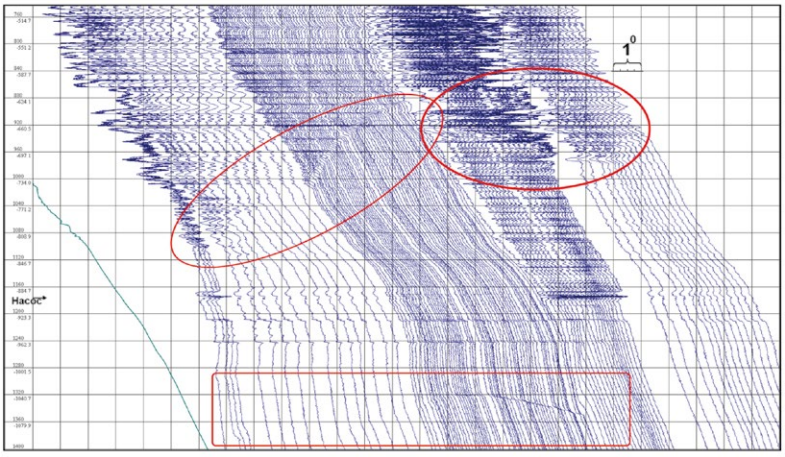


Рис. 5. **Уровень (выделено овалом) и ВНР (выделено прямоугольником) при остановке и работе ШГН**

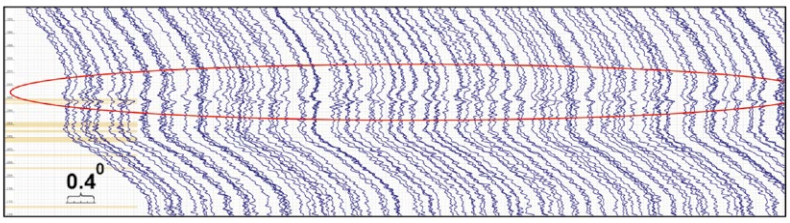


Рис. 6. **Приток газа из трещины ГРП**

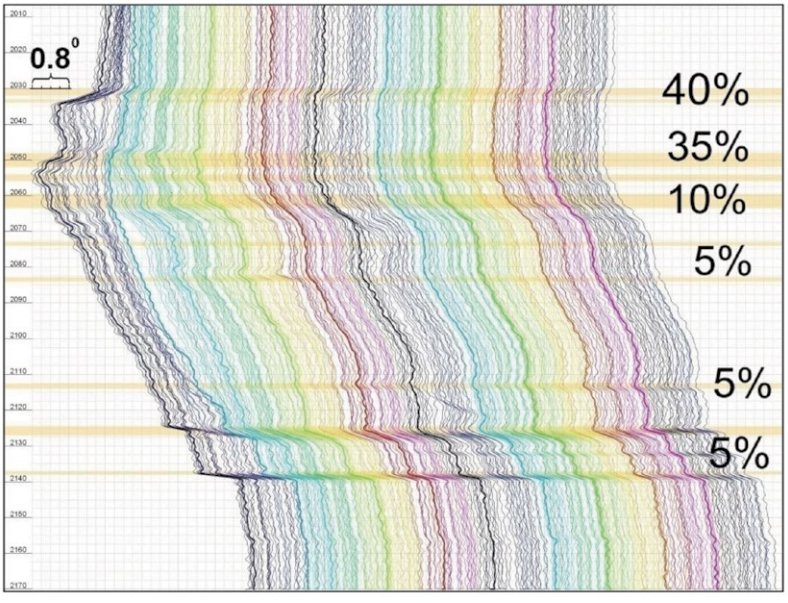


Рис. 7. **Разделение дебита по данным термометрии**

Следует отметить, что лучшим решением для определения состава поступающей жидкости было бы распределенное измерение давления или распределенные датчики состава. Работа в развитии этих направлений на сегодняшний момент выполнена не более чем на 30%. Реально работающие промышленные системы нам неизвестны. Ведутся работы на основе брэгговских решеток и распределенных электронных манометров.

Отдельно стоит затронуть тему определения притока газа. Поскольку дроссельный эффект при поступлении газа имеет отрицательное значение, определение пропластков, работающих газом, – задача, решаемая однозначно. В исследуемых нами скважинах был только один пример поступления газа. При этом дроссельный эффект наблюдался в трещине ГРП, и амплитуда его в скважине была низкой. Но на серии температурных кривых приток газа из трещины ГРП определяется однозначно (рис. 6).

3. ОВСт может определять дебит пластов (рис. 7). Точнее, по данным термометрии можно определить процентное соотношение дебитов различных пропластков или определить максимально и минимально работающие интервалы.

Однако точность и достоверность таких определений мала из-за сложной зависимости дроссельного эффекта от объема притока и наложения других термодинамических эффектов. Для увеличения точности измерений дебита необходимо осуществить нагрев кабеля на 2–3°С пропусканием через его токоведущие жилы электрического тока. Это позволит получить так называемый режим СТД и измерять степень охлаждения кабеля, которая зависит от объема притока.

Резюмируя все вышесказанное, можно утверждать, что имеющаяся технология уже сейчас позволяет решать задачи определения профиля притока и контроля работы скважины. Ее дальнейшая модификация с добавлением режима СТД и барометрии позволит решать эти задачи однозначно.

Сравним ОВСт с имеющимися технологиями.

Сравнение технологий

Сразу же надо обозначить, что в настоящее время развиты технологии профиля притока (ухода), которые выполняются на геофизическом кабеле. И область их применения – «лечение» скважин.

Т.е. технологии применимы тогда, когда извлечено насосное оборудование из скважин, скважина заглушена и цель работ – поиск проблемы, возникшей в скважине. Иногда ведется превентивный поиск проблемы перед спуском насосного оборудования. Существуют только два исключения – фонтанирующие скважины и скважины, оснащенные Y-tool. Причем при возникновении проблемы фонтанирующие скважины, как правило, перестают отдавать продукцию и их необходимо останавливать и «лечить».

ОВСт не смогут в ближайшее время составить конкуренцию комплексному прибору на кабеле. Суммарная стоимость оборудования существенно выше, а даже дополнительное оснащение ОВСт распределенным давлением и составом жидкости не позволит решать задачу на том же техническом уровне, что стандартный комплексный прибор. Следовательно, там, где «ходит» комплексный прибор, ОВСт менее эффективны.

Область действия ОВСт – мониторинг работы скважин. То есть область «профилактики», а не «лечения». И в ряде случаев у него нет альтернативы. Выделим основные преимущества:

- нет движущихся частей – мониторинг легко реализовать без участия геофизической партии, используя только системы передачи данных;
- получаемые данные не зависят от квалификации начальника партии и используемого прибора: проще организовать автоматическую обработку и принятие решений;
- отсутствуют стыковочные элементы и датчики: возможна работа в агрессивной среде весь межремонтный период и дольше.

В сравнении с Y-Tool ОВСт проигрывает в качестве измерений, преимущество только в контроле уровня жидкости. Однако оснащение всех скважин: замена парка ЭЦН и приобретение Y-Tool – задача более сложная и дорогая, чем оснащение скважин ОВСт.

Но что будет, если спустить комплексный прибор под насос и оставить его на забое на межремонтный период, проводя измерения по мере необходимости? В ОАО «Оренбургнефть» проводили подобные измерения, комплексный прибор не выдержал межремонтный период, а работа с ним требовала подъемника и партии ГИС. ОВСт в этом случае вне конкуренции.

Однако ОВСт и другие методы каротажа в процессе разработки применимы в большей части не для поиска возникших проблем со скважиной. Их назначение – управление работой месторождения. Управлять работой одной скважины или куста практически бессмысленно.

Определившись с областью применения ОВСт, перейдем к проблемам внедрения технологии.

Проблемы

Первая проблема – «болезнь» роста. Технологии оптоволоконной термометрии были «выброшены» на рынок «сырыми». Точность, чувствительность и разрешающая способность систем оказалась ниже уровня, необходимого для решения задач профиля притока. Приведем пример диаграмм именитых и не очень производителей, не называя их имен (рис. 8-9). Всю информацию можно найти в презентациях в интернете. Несмотря на высокие заявленные характеристики, реальные результаты далеки от решения задачи. «Шумы» на температурных кривых 1 и более °С, шаг по глубине – 1 м.

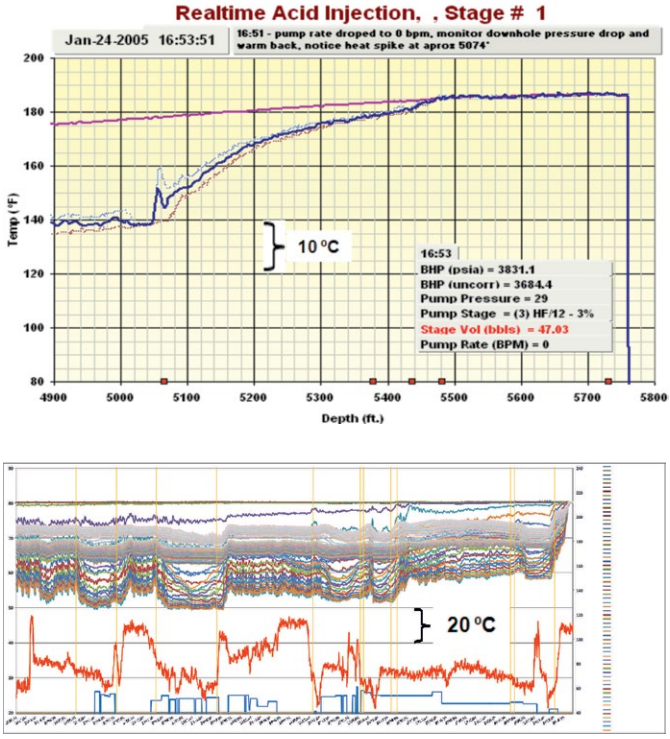


Рис. 8-9. **«Зашумленность» температурных кривых, грубая температурная шкала**

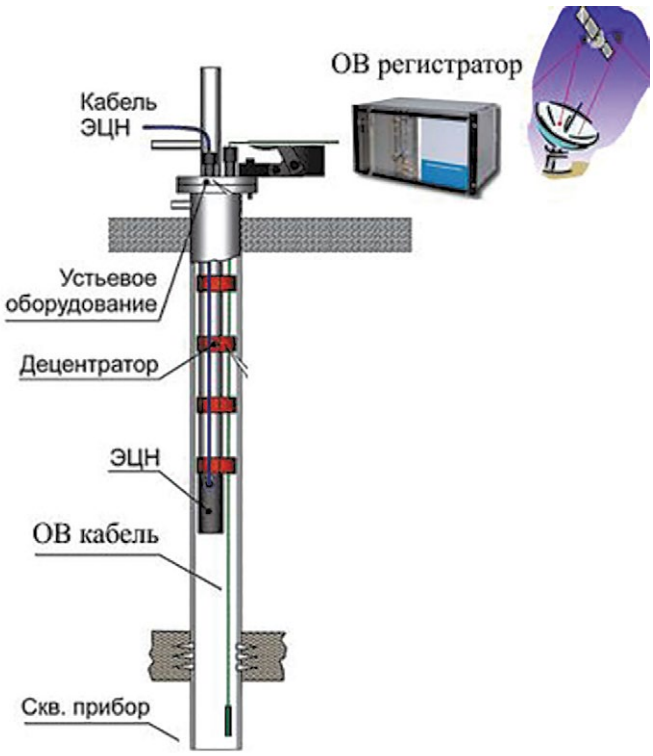
Какие параметры измерительной установки позволят решить задачу профиля притока в нефтяной скважине?

Во-первых, разрешающая способность по глубине (длине кабеля) **не больше 0.15 м**. Мы работаем с шагом по глубине 0.12 м, что позволяет фиксировать аномалии не менее чем тремя точками.

Во-вторых, чувствительность – **не хуже 0.1°С**. Аномалии дроссельного разогрева имеют амплитуду около 0.4°С. Мы работаем с чувствительностью 0.05°С, что позволяет уверенно фиксировать аномалии от работы пропластков и заколонных перетоков. В газовых скважинах допустима чувствительность **0.5 °С**. Обратите внимание на температурные шкалы рис. 2-4.

При этом время накопления – величина, тесно связанная с чувствительностью, – не должно превышать **15 мин.**, иначе не фиксируются переходные процессы. Для распознавания заколонных перетоков сверху пластов, работающих с малым дебитом на фоне высокодебитных, то есть «быстрых» задач, время накопления необходимо уменьшить до 30 сек.

Вторая проблема связана с областью применения каротажа в процессе разработки. Развитие систем контроля опередило развитие систем управления работой скважин и месторождения в целом.



Системы принятия решений просто не создавались. Вкладывать деньги в установку систем контроля без возможности управления и последующей оптимизации добычи неперспективно. Однако и оптимизировать разработку углеводородов без внедрения управляющих систем невозможно.

Третья проблема: кто создаст готовое решение, такое как «интеллектуальное месторождение»? Если иностранные компании, такие как Halliburton, Schlumberger, производят полный комплекс оборудования и услуг для нефтегазодобычи и имеют возможность изготовить и связать все компоненты в систему, то отечественных компаний, способных на такую интеграцию, не наблюдается. А по отдельности в разных компаниях создать системы контроля, управления и принятия решений не то что невозможно, но потребует очень много времени. Нефтегазодобывающие предприятия предпочитают купить готовое решение, а не вкладывать деньги в разработку.

В 2012-2013 годах только ленивый не рекламировал оптоволокно для нефтянки. На сайтах многих компаний до сих пор упоминаются «готовые» решения для мониторинга скважин, жаль только, что решений нет. Сейчас страсти поостыли, аппаратура оптоволоконной термометрии заняла свое место (исходя из технических характеристик) на контроле трубопроводов и электрических линий. Находит ОВСт применение при паронагнетании – технических характеристик «хватает».

В чем-то постоянное упоминание оптоволокна сыграло и отрицательную роль – из новшества оно превратилось в «неработающее старое».

Сухой остаток

Системы интеллектуальных скважин и интеллектуальных месторождений рано или поздно займут лидирующее положение в нефтегазодобыче. Это не дань моде, без этих систем невозможна оптимизация добычи.

Кто займет рынок услуг по оснащению месторождений – иностранные компании, инжиниринговые компании при нефтегазодобывающих предприятиях, объединение компаний – поставщиков услуг и оборудования, компании, выращенные в «бизнес – инкубаторах»? Однозначно тот, кто предложит лучший продукт и лучшее его продвижение!

Наша компания уже сейчас готова предложить сотрудничество по следующим направлениям:

1. Перфорация на депрессии с последующим мониторингом работы скважины. При этом перфорационная система и манометр спускается под ЭЦН или ШГН на оптоволоконном геофизическом кабеле совместно с глубинным насосом (рис. 10). Крепление к НКТ обеспечивает хождение кабеля. Далее перфорационная система позиционируется напротив пласта, насосом создается депрессия. Производится подрыв перфоратора и регистрируются давление. Далее перфоратор опускается на забой скважины, запускается насос и производится контроль работы пластов с помощью ОВСт и глубинного манометра весь период освоения. Определяются рабочие интервалы, интервалы поступления воды, гидродинамические параметры. Подбирается оптимальный режим работы насоса. После выхода скважины на режим геофизический кабель «сбрасывается» с подъемника и остается в скважине для последующего мониторинга работы, который рекомендуется производить ежеквартально или при смене производительности (продукции) скважины. **Преимущества: очистка пластов во время вскрытия, полностью контролируется работа пластов в эксплуатационном режиме без затрат времени на остановку и глушение скважины и ГИС.**

2. Контроль работы фонтанирующих скважин. Манометр спускается на оптоволоконном геофизическом кабеле с жестким креплением за НКТ. Контролируется выход скважины на режим, работа пластов, гидродинамические параметры. Подбирается оптимальный режим работы скважины. Кабель и манометр остаются в скважине весь межремонтный период. Единственная нерешенная задача – пакер с проходным отверстием под кабель.

3. Совместная разработка и внедрение услуг с применением ОВСт.

Дальнейшее развитие технологии ОВСт и наращивание ее дополнительными измерительными системами ООО «ПИТЦ «Геофизика» будет проводить уже после наработки достаточного количества скважин.

Список использованной литературы

Рыбка В.Ф. Результат применения оптоволоконных технологий распределенной термометрии при освоении скважины с помощью ЭЦН / Рыбка В.Ф. // Экспозиция нефть газ. – 2013. – №7 (32). – С. 13-16.

УДК 004.4

Проблемы внедрения технологии блокчейн

Problems of blockchain technology deployment

Г.Б. Маршалко[1]
G.B. Marshalko

КЛЮЧЕВЫЕ СЛОВА: блокчейн, криптовалюта, биткойн, информационно-телекоммуникационные системы, хэширование, доказательство полномочий, безопасность протоколов, доказательство работы.

АННОТАЦИЯ: Настоящая статья анализирует становящуюся все более популярной в настоящее время технологию блокчейн, которая, как следует из материала, является ярким примером поиска новых парадигм взаимодействия в цифровом мире. Статья рассматривает феномен криптовалюты как единственный реально состоявшийся пример применения блокчейна. Исследуется архитектура систем, реализующих криптовалюты, специфические условия их построения, в том числе отсутствие единого управляющего центра, анонимность пользователей, объективная необходимость использования координирующего механизма.

KEYWORDS: blockchain, crypto, bitcoin, information and telecommunication systems, hashing, proof-of-authority, security of protocols, proof-of-work.

ABSTRACT: This article analyzes the now becoming increasingly popular blockchain technology, which, as follows from the material, is a vivid example of the search for new paradigms of interaction in the digital world. The article examines the phenomenon of the cryptocurrency as the only real-life example of the use of the blockchain. The architecture of systems implementing cryptocurrencies, specific conditions for their construction, including the absence of a single control center, the anonymity of users, the objective necessity of using a coordinating mechanism is considered.

Появление новых информационных технологий всегда несет не только новые возможности по оптимизации процессов взаимодействия, но и сопровождается появлением новых угроз безопасности, которые в случае их игнорирования могут свести к нулю потенциальные выгоды от внедрения таких технологий. Своевременная оценка таких угроз и выработка адекватных мер противодействия является краеугольным камнем развития информационно-телекоммуникационной области.

Широко обсуждаемая в настоящее время технология блокчейн является ярким примером попытки поиска новых парадигм взаимодействия в цифровом мире. Единственным реально состоявшимся примером применения блокчейна на настоящий момент, по сути, являются криптовалюты. Архитектура систем, реализующих криптовалюты, построена исходя их достаточно специфических условий, в которых они используются, а именно: отсутствие единого управляющего

[1] Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), ISO TC 307 «Blockchain and distributed ledger technologies»

Рис. 1. Диаграмма выбора варианта блокчейна для реализации. *Закрытый частный блокчейн* – доступ к реестру (чтение и запись) имеют только авторизованные пользователи. *Закрытый публичный блокчейн* – запись могут осуществлять авторизованные пользователи, чтение могут производить все пользователи. *Открытый публичный блокчейн* – доступ к реестру имеют все пользователи.

центра, анонимность (или псевдонимность пользователей). В этом случае необходимо использовать механизм, который может заменить традиционно используемую для обеспечения взаимодействия между пользователями доверенную третью сторону (администратора).

Такой механизм, реализованный, например, в криптовалюте биткойн, использует общедоступный распределенный или точнее реплицированный (т.е. находящийся в идентичных копиях у пользователей) реестр произведенных в системе операций. Реестр построен таким образом, чтобы в него было вычислительно сложно внести изменения. Это достигается посредством использования криптографических механизмов при формировании реестра: функций хэширования и электронных подписей. Поскольку в системе отсутствует администратор, который уполномочен вносить изменения в реестр, то используются т.н. механизмы консенсуса. По сути, это некоторые вероятностные алгоритмы (т.е. алгоритмы, время выполнения которых не детерминировано), которые позволяют выбрать временного администратора для выполнения текущей операции. На практике в качестве таких алгоритмов используются алгоритмы нахождения решения некоторых вычислительно сложных математических задач, например, нахождения значения хэш-функции из заданного диапазона (т.н. методы доказательства работы, Proof-of-work).

Попытки же применения блокчейна в других областях, связанных с уже существующими финансовыми и правовыми отношениями (регистрация прав, контроль за движением товаров и прочее), сталкиваются с тем, что подобные архитектурные решения не адекватны стоящей перед разработчиком задаче, что требует изменения структуры системы и логики ее работы. Например, необходимость аутентификации абонентов делает излишним применение описанного выше механизма консенсуса, использующего метод доказательства работы, взамен которого используются, например, механизм византийского соглашения или доказательства полномочий (Proof-of-authority).

В этой связи наибольшей проблемой для технологии блокчейн являются массовые попытки ее внедрения там, где это нецелесообразно. Дело в том, что для большинства современных вариантов ее применения ответ на вопрос, возможно ли реализовать аналогичную систему без блокчейна, будет положительным. Более того, как показывает проведенный к настоящему моменту ана-

лиз, децентрализованный блокчейн в своем современном виде не подходит для использования в масштабных высоконагруженных системах, вследствие естественных ограничений по производительности (сложности достижения консенсуса и необходимости хранения больших объемов данных).

В случае использования его централизованных (частично централизованных) вариантов характеристики информационных систем получаются хуже, чем характеристики систем, используемых в настоящее время. На рис. 1.[2] приведена диаграмма выбора того или иного варианта блокчейн-систем в зависимости от требуемого функционала.

С точки зрения вопросов информационной безопасности необходимо рассмотреть два аспекта безопасности блокчейна: теоретический и практический.

Теоретический, прежде всего, связан с общей научной непроработанностью обоснования безопасности протоколов консенсуса. Для наиболее старого, используемого в криптовалюте Биткойн, протокола Proof-of-Work к настоящему моменту предложено большое количество различных атак, некоторые из которых достаточно просто могут быть реализованы практически. Большинство из них связано с отсутствием управляющего центра и основано на воздействии на сетевые протоколы и изменении параметров внутреннего трафика сети. В этом случае нарушитель тем или иным способом воздействует на сеть, модифицируя или перенаправляя передаваемые пакеты таким образом, чтобы, например, лишить атакуемого пользователя доступа к копиям истинного реестра и возможности проверки транзакций. Также узлы, занимающиеся подтверждением транзакций (майнеры), могут действовать вопреки правилам системы, например, аккумулируя большие вычислительные мощности (т.н. атака 51%), что позволяет получать возможность управления системой.

[2] K. Wust, A. Gervais, Do you need a Blockchain?

Другие варианты достижения консенсуса, такие как доказательство владения долей (Proof-of-stake, Delegated Proof-of-stake), доказательство владения дисковым пространством Proof-of-space, или обладают еще большим набором уязвимостей, или слабо изучены.

В целом на настоящий момент непонятно, каким должен быть безопасный протокол консенсуса с тем, чтобы обеспечивать стабильное функционирования блокчейн-системы продолжительное время с учетом возможного воздействия нарушителей.

С практической точки зрения разрабатываемые энтузиастами современные блокчейн-системы

зачастую обладают серьезными уязвимостями, которые позволяют проводить хакерские атаки. Это в большей степени справедливо для области криптовалют. Широко известны атаки на криптовалютные биржи и отдельных пользователей, направленные прежде всего на кражи данных криптовалютных кошельков: Mt. Gox, Bitfinex, IOTA и др.

Необходимо отметить, что декларируемая децентрализованность блокчейн-систем во многом условна. Прежде всего, проблема централизации возникает вследствие наличия достаточно узкого круга разработчиков используемых протоколов и программного обеспечения, определяющих логику работы системы, что показывает история развития таких систем, как Биткойн и Эфереум. В связи с этим современные исследователи[3] вводят понятия «управление с помощью инфраструктуры», подразумевая концепцию, согласно которой в логику работы системы может быть заложен алгоритм, который будет регулировать функционирование системы, и «управление инфраструктурой», т.е. когда разработчики управляют системой через изменение логики его работы.

Попытка использования блокчейна вне замкнутой цифровой среды, например, для регистрации объектов недвижимости, контроля за движением товаров, ставит вопрос юридической значимости регистрационных действий. Даже не рассматривая нормативные и организационно-технические вопросы применения электронной подписи, критическим в таком случае является вопрос достоверности регистрации в системе событий или объектов, происходящих в реальном (физическом) мире. Это крайне проблемный вопрос и для существующих систем, и для технологии блокчейн. На сегодняшний момент отсутствуют доверенные способы такой (автоматической) регистрации. Ряд исследователей связывают вопрос внедрения блокчейн именно с решением задачи разработки таких способов.

[3] P. De Filippi, B. Loveluck, The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure.

SUMMARIES

INFORMATIONAL SECURITY

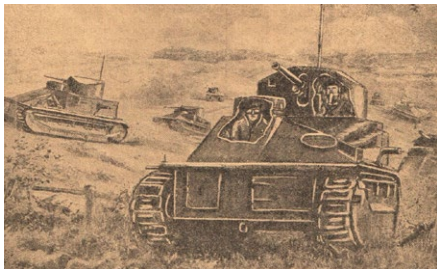
The issues of informational security, resistance against cyber crime and development of informational infrastructure of the government become more and more currently central and discussed on the highest level. For example, it became the main subject of a conference of the Security Council chaired by Vladimir Putin in October that took place in the Kremlin, or a conference in Sochi dedicated to the new electronic financial instruments. According to Vladimir Putin, we have to predict threats with a current reaction on it and to develop national production base.

THE NATIONAL ELECTRONIC COMPONENT BASE

In the Rosoboronexport there was held a meeting of the Coordinating Council of Developers and Manufacturers of Radioelectronic Equipment, Electronic Component Base (ECB) and Machine Building Products of the Russian Engineering Union and Section 4 of the IAB ECB under the Board of the Military-Industrial Commission of the Russian Federation. The main topic of the discussion was the enforcement of legislation on restrictions and prohibitions on the admission of imported electronic products.

HIGH CURRENCY

'The leader of Microsoft declares that Democratic People's Republic of Korea stands behind the cyber attack WannaCry.' The Great Britain authorities accused Iran in a cyber attack on the parliament". "Minister of Defense in Poland speaks about 'dealing with an attack' from the foreign countries.' 'This is madness': Russia answered to the USA accusations in using the soft 'Kaspersky Laboratory' for espionage.' Here are the headlines of informational agencies published just within two days in the middle of October. The mentioned subjects are obviously similar: everything is about real threats than includes aggressive actions of IT-groups directed against several companies, industrial sectors and even against the whole countries in this uneasy day and age of hybrid oppositions.



WHAT WAS 'RADIOFRONT' WRITING ABOUT IN 1937

Soviet radio is not only a propagandist, agitator and organizer of a new way of life. It's the most pointed and versatile instrument of the class war in the hands of proletariat. Radio fights for a financial plan within the companies, it fights against the mill cog, organizing the kolkhoz fields. Radio works all day and night and fights for the general party line every hour. The saboteurs couldn't leave this branch of our construction without their attention. Technically they were able to make a mess: they brought chaos into the air. Leading of the whole direction of soviet radiofan work have stayed in hands of the indifferent to politics specialists for years.

UP CLOSE: PAVEL KHILOV

We are the Russian organization specialized on the expertise in a way of forming national politics regarding different aspects of using informational technologies in the authorities. The work of an Expert center is focused on the development and implementation of the electronic technologies of the government on different levels of authorities and it is also focused on supplying an independent public control on this important process. The Expert center unites more than a hundred experts in the main lines of Informational and Communication Technologies development.

CONSORTIUM 'THE SMART CITY'

The memorandum about creating the National consortium of the digital technologies development and implementation in the city department (consortium 'The smart city') was signed during the Sixth international forum of innovational development 'Open innovations' in Moscow. The work on creating "the smart cities" is going on as part of the 'Russian Federation digital economy' program realization. This program was confirmed by the order of the Russian Federation government №1632-p from 28th of June 2017. The program was prepared by the Russian Ministry of Communications along with the experts and institutes of development. Creation and realization of the 'smart cities' conception on the Russian Federation territory is one of the primary targets of the consortium.

HANNOVER MESSE

23–27 апреля 2018
Ганновер ■ Германия

hannovermesse.com #hm18

HERGESTELLT IN MÉXICO PARTNER COUNTRY 2018

Совместно с HANNOVER MESSE 2018

CeMAT

Информация
о посещении и участии
+7 495 669 46 46
info@messe-russia.ru

Deutsche Messe

Get new technology first

HANNOVER MESSE

ОРГАНИЗАТОР

МИНИСТЕРСТВО ОБОРОНЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

2018

ARMY

МЕЖДУНАРОДНЫЙ ВОЕННО-ТЕХНИЧЕСКИЙ ФОРУМ «АРМИЯ-2018»

21–26 АВГУСТА
ПАТРИОТ ЭКСПО

WWW.RUSARMYEXPO.RU

ВЫСТАВОЧНЫЙ ОПЕРАТОР

МКВ

МЕЖДУНАРОДНЫЕ КОНГРЕССЫ И ВЫСТАВКИ