ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЖУРНАЛ

КАРТ БЛАНШ

ПЛАТЕЖНАЯ ИНДУСТРИЯ ИННОВАЦИИ

1-2 (135-136)'2016
www.smart-payments.info

Tempus

2014 2016 CABRIOLET

R&D БИЗНЕС: ОДНА МЕДАЛЬ НА ДВОИХ

7event
group

КАЖДОЕ МЕРОПРИЯТИЕ –
ЗНАЧИМОЕ СОБЫТИЕ
В ДЕЛОВОЙ ЖИЗНИ СТРАНЫ




7event Group – группа компаний обеспечивает:

- Профессиональную организацию деловых мероприятий;
- Разработку, сопровождение и реализацию проектов;
- Организацию и взаимодействие участников мероприятий;
- Предоставление экспертной и аналитической поддержки.

Проекты 7event Group – укрепление взаимоотношений между:

- бизнесом;
- властью;
- институтами развития;
- профессиональными сообществами;
- общественными организациями.

7event Group – группа компаний:

- IT Альянс – Образование. Индустрия. Наука;
- ИА журнал «Карт Бланш» – технологии, инновации;
- компания «Финансовая студия» – консалтинговая компания.

7event Group:

Организация отраслевых мероприятий + обеспечение аналитической и экспертной поддержки + освещение в прессе = значимое событие отрасли

Тел.: +38 (095) 356-99-69; +38(067) 375-76-37
E-mail: marina.medinskaya@it-alliance.org.ua oksana.hahina@it-alliance.org.ua

СОДЕРЖАНИЕ

КАРТ БЛАНШ
КАРТОЧНЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

№ 1-2•2016

Информаційно-аналітичний журнал

Виходить у світ з грудня 2001 р.

Засновник та видавець:
Олена ГОЛЕМБОВСЬКА

Выпуск журнала поддержан европейским проектом TEMPUS-CABRIOLET Model-Oriented Approach and Intelligent Knowledge-Based System for Evolvable Academia-Industry Cooperation in Electronic and Computer Engineering (2013-2016).

Адреса редакції:
м. Київ, Україна

Тел.: +380 44 248 0416
www.smart-payments.info

Свідоцтво про реєстрацію
КВ №11758-629ПР
від 19.09.2006
Передплатний індекс
23741

Кольороподіл та друк:
ТОВ «Юстон ЛТД»
вул. Олеся Гончара, 36а,
м. Київ, Україна, 01034

Тираж **1000 прим.**

Ціна – договірна

Підписано до друку 11.05.2016

Елена ГОЛЕМБОВСКАЯ

Основатель
и главный редактор
Журнал «Карт Бланш»
Соорганизатор CYBER
FORUM DESSERT
B2S-S2B 2016

Уважаемые коллеги, друзья и читатели журнала!

У вас в руках эксклюзивный, не побоюсь этого слова, номер журнала «Карт Бланш». Его эксклюзивность состоит в том, что, во-первых, это первый в Украине выпуск, полностью посвященный теме R&D (Research&Development), выход которого приурочен к масштабному международному мероприятию – CYBER FORUM DESSERT B2S-S2B 2016 (18-23 мая). И вторая его особенность – интернациональность и многоязычность. Статьи выпуска, в подготовке которых приняли участие авторы разных стран (Великобритании, Канады, Греции, Италии, США, Украины, Швеции, Эстонии), написаны на украинском, английском и русском языках.

Самые ключевые открытия последнего времени в таких сумасшедших областях, как телепортация, вейвлет-анализ, квантовые компьютеры и другие, были сделаны в R&D лабораториях известнейших компаний – General Electric, IBM, Bell Labs, Lucent Technologies и других. Будущее – за совместной деятельностью науки, образования и бизнеса, и доказывать это в последнее время нет смысла.

Выглядит символичным, что в то время, когда бизнес максимально сокращает свои рекламные бюджеты, этот выпуск журнала поддержан европейским образовательным проектом TEMPUS-CABRIOLET, о котором подробнее мы расскажем дальше. И в этом видится знак того, что именно науке будет принадлежать роль драйвера инновационных процессов во всех отраслях. Хочется верить, и для этого есть все предпосылки, что Украина, имея огромнейший потенциал, займет свое почетное место среди мирового инновационного сообщества.

А потенциал такой, пройдемся по цифрам. Украина занимает 30 место по уровню образования в рейтинге* стран мира из 187, и это очень неплохо! По уровню расходов на образование в рейтинге стран мира занимает 57 позицию из 153. В рейтинге глобальной конкурентоспособности – 79 из 140, по размеру внутреннего валового продукта – 59 из 193, по индексу человеческого развития Украина попадает в группу с высоким уровнем развития и занимает там 81 позицию из 188, в рейтинге стран мира по индексу счастья находится на 123 позиции из 157. А вот в рейтинге лучших университетов мира (TOP200), по версии Times Higher Education, ни одного украинского университета, к сожалению, нет. Так что работы в этом направлении много.

Как известно, одна из возможностей реализации потенциала страны – это вложение инвестиций в развитие сектора R&D. В 2016 году Америка увеличила инвестиции в R&D направление на 3,4% до $514 млн. Китайские вложения в R&D рынок увеличились на 6,3% до $396 млн. Азиатский R&D продолжает свое наступление и занимает уже в мировом рынке долю около 42%. Информацией о том, как выглядит прогноз всемирных инвестиций в R&D в 2016 году, мы хотим поделиться с читателями на 23 странице этого номера (2016 Global R&D Fundidng Forecast**). Где-то на этой карте есть место и Украины. Давайте поможем вместе его найти.

Существует расхожее словосочетание: две стороны одной медали. Оно очень символично для темы R&D, кооперации науки и бизнеса, университетов и индустрии. Такую медаль, объединяющую эти сущности, очень нужно получить Украине в гонке умов, технологий и экономик

Пользуясь случаем, я от себя лично и от имени редакции журнала, хочу поблагодарить всех, кто принял участие в подготовке и поддержке выпуска, а также автора R&D-идеи номера и соисполнителя этого проекта Вячеслава Харченко, без идейной и организационной работы и помощи которого R&D-выпуск не состоялся бы. И надеюсь на то, что этот номер станет стартовой площадкой и местом для обсуждений, обмена опытом, получения важной информации и формирования R&D бизнес-сообщества, которое создает и приближает будущее.

Далее я приглашаю к слову Вячеслава Харченко.

С уважением,
Елена Голембовская

* Все приведенные данные взяты из разных отчетов, опубликованных Центром гуманитарных технологий (ISSN 2310-1792) на сайте http://gtmarket.ru.

** 2016 Global R&D Fundidng Forecast Source: R&D Magazine, Industrial Research Institute and Research-Technology Management. http://www.rdmag.com/topics/global-r-d-funding-forecast.

R&D: ОТ КАДРОВОЙ К ТЕХНОЛОГИЧЕСКОЙ ПАРАДИГМЕ КООПЕРАЦИИ УНИВЕРСИТЕТОВ И ИНДУСТРИИ

Этот номер журнала «Карт Бланш» выходит в преддверии CYBER FORUM DESSERT B2S-S2B 2016 http://www.dessertcon.com/, который будет проходить 19-20 мая 2016 года в Киеве и является частью юбилейных событий, посвященных десятилетию конференции «Dependable Systems, Services and Technologies» (DESSERT2006-2016) и проводимых 17-23 мая последовательно в Харькове, Киеве, Черновцах. Одна из важных тем Форума – развитие кооперации науки, образования и ИТ-индустрии в рамках концепции B2S-S2B (бизнес для науки – наука для бизнеса). Тема кооперации не нова и уже набирает темп в Украине – по крайней мере, она регулярно обсуждается, нарабатываются успешные и не очень практики. ИТ-сообщество понимает, что университетам без такой кооперации не выжить в хорошем – конкурентном смысле этого слова, а бизнесу просто не существовать без кадровой подпитки. Университеты и индустрия прошли этап (первый!) определенной неразберихи, взаимных претензий и вошли в фазу поиска путей взаимовыгодной кооперации (этап второй!). Учитывая, что украинский ИТ-рынок на 90 процентов (или более) аутсорсинговый, то получается эти 90 (существенное большинство) процентов настроены исключительно на кадровую парадигму кооперации. 10 или менее (?) процентов компаний являются продуктовыми и имеют R&D (Research and Development) компоненту.

А что университеты? Здесь можно выделить три группы: первая пока еще не работает даже по ней («студенты и сами устроятся»), вторая – выстраивает модель кооперации А («кафедра – гнездо кодеров-девелоперов»), третья – не хочет оставаться в рамках (только) этой модели, а движется к более инновационным моделям – B, C (мы писали об этом в предыдущих номерах журнала Карт Бланш №8-9'2012, №3-4'2015. Понятно, что Украине без аутсорсинговой компоненты не обойтись в ближайшие десять лет (она есть во всех и более продвинутых ИТ-индустриях) и профессия аутсорсингового айтишника будет оставаться и развиваться как массовая в хорошем смысле слова.

А что дальше? Стране надо выходить на «постиндустриальный» (третий!) этап развития ИТ-отрасли, а следовательно, и кооперации. Давайте вернемся к концепции B2S-S2B. Еще раз подчеркнем, что речь идет о кооперации науки и бизнеса, причем науки прикладной, технологической, «продаваемой». Технологии, создаваемые в университетах совместно и для индустрии, уже устоявшаяся практика в мире. Таким образом, технологическая парадигма кооперации должна гармонично дополнить кадровую. И в этой области в Украине есть много удачных примеров, однако эти примеры не слились в эффективную систему, поддерживаемую государством.

В рамках этой темы мы хотели бы основное внимание уделить обсуждению перспектив, барьеров и драйверов развития сегмента R&D в контексте национальных интересов Украины, европейского и мирового трендов, сотрудничества в одном из наиболее инвестиционно привлекательных секторов экономики. Обсуждение планируется провести в рамках тематического трека киевской части Форума, посвященного R&D, и семинара-тренинга в Черновцах (WS BASIC). Их цель – активизировать развитие этого сегмента, что позволит, во-первых, стать Украине одной из ведущих стран мира не только по ко-

Вячеслав ХАРЧЕНКО

Профессор,
докт. техн. наук

личеству квалифицированных ИТ-специалистов и объему выполняемых аутсорсинговых проектов, а и по количеству создаваемых и продаваемых продуктов (технологий); во-вторых, перейти на качественно новый уровень кооперации образования, науки и бизнеса; в-третьих, что крайне важно, облегчить решение проблемы сохранения молодых и талантливых кадров в университетах, гармонизируя их творческие амбиции, академическую свободу и финансовые условия работы.

Предлагаемые темы для обсуждения:

- Анализ состояния мирового, европейского и национального R&D рынка.
- Барьеры (мотивационные, организационные, финансовые) и драйверы R&D для бизнеса и университетов и их кооперации.
- Анализ и пути имплементации лучших национальных и международных практик.
- Особенности развития R&D в сфере ИТ-безопасности и др.

Для того чтобы сделать обсуждение и дальнейшие шаги более результативными, мы предлагаем Вашему вниманию выпуск журнала «Карт Бланш», в котором опубликованы статьи специалистов в этой области, достигших успехов и имеющих свое видение этой области. Среди авторов – аспиранты и академики, профессора и менеджеры, работающие в университетах и индустрии и представляющие разные страны (Великобританию, Канаду, Грецию, Италию, США, Украину, Швецию, Эстонию). Представленные статьи объединены в несколько тематических групп:

- R&D: от «тигров» к университетам;
- Как стартовать в R&D;
- Наука, кадры для R&D;
- R&D для ИТ-безопасности.

Выпуск журнала поддержан европейским проектом TEMPUS-CABRIOLET Model-Oriented Approach and Intelligent Knowledge-Based System for Evolvable Academia-Industry Cooperation in Electronic and Computer Engineering (2013-2016), выполняемым консорциумом британских, испанских, итальянских, португальских и украинских университетов, академических институтов и компаний.

Вячеслав Харченко
Председатель
CYBER FORUM DESSERT B2S-S2B 2016
Заведующий кафедрой компьютерных систем и сетей Национального аэрокосмического университета им. М.Е. Жуковского «ХАИ»,
национальный координатор проектов TEMPUS-GreenCo, SEREIN, CABRIOLET

ABOUT TEMPUS-CABRIOLET

Model-Oriented Approach and Intelligent Knowledge-Based System for Evolvable Academia-Industry Cooperation in Electronic and Computer Engineering (2013-2016)

The publishing of the Carte Blanche journal volume is partially supported by EC-funded TEMPUS-CABRIOLET Model-Oriented Approach and Intelligent Knowledge-Based System for Evolvable Academia-Industry Cooperation in Electronic and Computer Engineering, 2013-2016.

CABRIOLET is aimed on introduction of model-oriented approach for effective academia-industry cooperation in Electronic and Computer Engineering, developing intelligent knowledge-based system for supporting the model-oriented approach and launching cloud-based web-portal as communication mechanism between involved parties.

The project address the society demand on high qualified engineering specialists by introducing innovative methodology for smooth and productive cooperation between academia and industry in the computer and electronics engineering domains.

The project is developing by the consortium of partners from UK, Sweden, Italy, Portugal and Ukraine. Ukrainian academic and non-academic partners have joined the consortium to cover all Ukrainian regions and all major domains of computer and electronic engineering.

R&D: ОТ «ТИГРОВ» К УНИВЕРСИТЕТАМ

- R&D и бизнес-сообщество
- Креативность и инновации
- University-Industry R&D Cooperation

THE ENTERPRISE SOCIETY – A VIEW FROM AN ASIAN TIGER

According to the Ministry of Trade and Industry Singapore website: «Our vision is for Singapore to be a leading global city with a dynamic economy, world-class enterprises and innovative and productive SMEs. Singapore will over a conducive environment for entrepreneurs and enterprises to tap its diverse opportunities, and provide good jobs which are attractive to talent at all levels.» Let's start to unpick this and investigate that «conducive environment».

Singapore, which translates as The Lion City, or the little red dot as it is sometimes known, is a diamond-shaped island at the bottom end of Peninsular Malaysia, measuring around 50 kilometres in one direction and 27 kilometres in the other, with a population approaching 5.5 million people, and is just one degree North of the equator. Singapore has relatively few natural resources, it still relies on pumping some of its freshwater supply from Malaysia, and the size of the island has increased via a process of land reclamation by over 20% since the nation state was established in 1965.

The Singapore economy is, therefore, heavily dependent on its human resources. Traditionally this was based on entrepot (import/export) trading. Singapore's main industries are now financial services, manufacturing, and oil-refining. The view of the downtown skyline from the top floor of the astonishing ship-shaped structure that is the Marina Bay Sands Hotel is studied with skyscrapers occupied by multinational companies, such as the Overseas Union Bank. Not far away are the Keppel Shipyards, and further away again, Jurong Island, the home of Singapore's petrochemical industry. Almost everywhere you travel in Singapore you will encounter construction work encompassing new Mass Rapid Transit (MRT – i.e. Metro) lines, public Housing Development Blocks and private condominiums, new roads and flyovers, and, of course, yet more shopping malls (Singapore's main pastime is said to be shopping). Even though there has been a recent slowdown in the economy, this is not evident on the streets of Singapore, and the impression is of a truly dynamic economy.

The idea of the development of talent is in-bred into the Singapore psyche. Education is seen as the basis on which to build young entrepreneurs, and school kids of all ages are strongly encouraged, some might same driven, by their parents to excel in everything they do, in academic studies and extra-curricular activities. Parents themselves are prepared to go back to school so that they can support their children with their studies. It is not unknown to walk around Singapore and see teenagers sporting T-shirts bearing logos such as «I'm an Entrepreneur», such is the culture that exists there.

There are now five universities in Singapore, with the National University of Singapore (NUS) and Nanyang Technological University (NTU) coming in at very respectable positions of 12th and 13th in the QS World University Rankings 2016. Around two years ago the Singapore Government announced the establishment of the country's fifth (excluding foreign campuses) university, the Singapore Institute of Technology, with vision to be «A leader in innovative university education by integrating learning, industry and community» and an emphasis on developing industry-ready graduates. Going forward, SIT is working with a number of overseas partners and plans to offer joint degrees as well as its own. Central to all programmes will be the requirement that students must spend 8-12 months on an Integrated Work Study Programme – an internship – giving students an opportunity to develop soft skills, in areas such as teamwork, communication and project planning.

An alternative for high-school graduates is to enrol in one of the five Singapore polytechnics, which very much aim to prepare students to contribute to Singapore's economic development with an emphasis on developing their practical, as well as theoretical, skills. A third option is the Institute of Technical Education, with an emphasis on vocational training.

An essential component of the «conducive environment» is the Agency for Science, Technology and Research (A*STAR), which works closely with local universities, providing a bridge between industry and academia. A*STAR includes the Biomedical Research Council and the Science and Engineering Research Council. Physical support for A*STAR includes two purpose-built buildings in

Chris PHILLIPS

Prof., Head of Academic Operations Singapore, Newcastle University, United Kingdom

close proximity, Biopolis, a research and development centre for biomedical sciences, and Fusionopolis. These are not just science parks in the conventional sense, but complete environments including shopping malls and housing.

It is unlikely that any of this would have happened without significant government involvement. The architect of the foundations of the Singapore economy was the visionary leader Lee Kuan Yew, who died just over a year ago. Today it is his son, Lee Hsien Loong, who leads the government. In a speech at a Smart Nation Singapore Reception held in March 2015 Prime Minister Lee said «We are investing in R&D, over the past ten years we have invested SGD 30billion, we have grown research institutes that work with companies to develop new solutions.» Supporting these developments are a number of government agencies, including The Economic Development Board and the Workforce Development Agency. The government has established LaunchPad offering facilities for start-up companies in the biomedical sciences and electrical and electronic areas to be nurtured and flourish. The same political party, the People's Action Party, has been in office since Singapore became an independent country in 1965, providing more stability than in most other countries, with five-year strategies being employed to plan the economic infrastructure.

Singapore has a truly eclectic mix of both permanent and temporary inhabitants. The local population is predominantly of Chinese ethnicity, with the other main races being Malay and Tamil. However there is a significant ex-pat population, including Western Europeans, Australians, and Americans. Singapore has introduced special categories of residency to promote inward migration,

The Singapore CBD skyline

The Singapore CBD skyline

including Permanent Resident and Employment Pass Holders, and this has led to an inward flow of talent from all over the world. Although the official language of Singapore is Malay, the medium of instruction at all levels of education is English, and this is the lingua franca of all business activity. Singapore is recognised as one of the least corrupt countries in the world. In the Singapore suburbs you will regularly see signs warning about bicycle thefts, and money and sex scams, but the reality is that the crime rate is very low, although the mantra 'low crime does not mean no crime' is taken seriously by all local residents. All of this, along with the development of the local employee base, combines to make Singapore a very attractive location for inward investment by foreign countries, and a place that foreign employees would like to work in.

So, has all of this been effective? Some notable Singapore inventions are the Creative Labs Soundblaster sound card, the Trek Technology thumb drive – the original USB stick, and the match.com dating site. (And, of course, the Singapore Sling cocktail.)

Singapore faces many of the issues of most other countries in the world, not least the challenges of an ageing population, increasing obesity, etc. However the underlying physical, societal, and most importantly, governmental attitudes to meeting these challenges, twinned with the inherent entrepreneurial spirit of its citizens, means that Singapore is well-placed to meet those challenges and continue to grow as a leading global financial, commercial and transport hub. Singapore is certainly unique, and is unlikely to be replicable elsewhere, but there are lessons here for us all to learn from. ■

Photos by Angela Sewell

KTH AND KHAI: FACILITATING CLIMATE OF CREATIVITY AND INNOVATION

Sweden is considered to be one of the most technologically innovative countries in the world and Stockholm is consistently ranked as one of world's most entrepreneurial, innovative and attractive cities.

Swedish academic community maintains close relationship with the continuously expanding network of multinational technology-intensive companies offering opportunities for students and researchers to study and carry out their research in this fruitful environment.

KTH Royal Institute of Technology (Kungliga Tekniska Hogskolan, KTH) was founded in 1827 and is the largest engineering university in Sweden. KTH is responsible for one-third of Sweden's capacity for engineering studies and technical research at post-secondary level.

The five KTH campuses in Greater Stockholm, gather more than 12,000 full-time students, some 1,800 PhD students and approximately 3,700 full-time employees. The campuses are strategically located close to their areas of research and study, for example KTH Kista is situated in the middle of the Kista ICT hub, with some of the world's leading Information and Communications Technology companies.

KTH is working with industry and society in the pursuit of sustainable solutions to some of humanity's greatest challenges: climate change, future energy supply, urbanisation and quality of life for the rapidly-growing elderly population. KTH is addressing these with world leading, high-impact research and education in natural sciences and all branches of engineering, as well as in architecture, industrial management, urban planning, history and philosophy. Almost two-thirds of the SEK 4 billion turnover relates to research.

Basic and applied research activities are performed side-by-side at KTH and interdisciplinary research is conducted in parallel with work in specific fields. This approach encourages versatile solutions and the innovative climate creates many opportunities to realise great ideas. Its educational programmes foster a new generation of engineers, architects, teachers and undergraduate engineers.

KTH embraces academia and the public and private sectors working together. It is a part of extensive international research collaborations including a large number of educational exchange or joint programmes with universities and colleges in Europe, the U.S., Australia, Asia and Africa.

The wide spectrum of research demands variation in focus, approach and formation. KTH staff works on creation of an open atmosphere and breaking down traditional barriers between academic disciplines. Basic research is conducted in parallel with applied research, and the same is true of multidisciplinary work and specifically targeted work.

Based on strong areas of research at KTH, five focus areas have been created. These work as platforms for multidiciplinary research: Transport, Life Science Technology, Materials, Information and Communication Technology, Energy.

Close collaboration with society and industry creates a natural arena and better conditions for the practical implementation of research results and researchers have the opportunity to see their ideas make a tangible impact in society.

KTH contributes to sustainable development by providing educational programmes, conducting research and by interacting with the surrounding community. Through its activities, KTH also impacts the environment in practi-

cal terms through the consumption of materials and water, energy and chemicals, travel and transport and construction, and indirectly through purchasing and procurement.

The Division of Industrial Ecology at KTH is active in the new multidisciplinary field of Industrial Ecology. The division is responsible for the main part of the environmental courses given at KTH for all engineering programs. The Division is running an International Master Program in Sustainable Technology. The Division is a co-coordinator of Erasmus-Mundus SDPROMO project and a European network «Capacity building in Sustainable Development». There are also several distance learning courses for industry and authorities. KTH has a long-term cooperation with all participated partner Universities from the third countries, funded by European Commission (Tempus, Tacis CBC, Interreg and Asia-Link) as well as national funds (SI and SIDA).

KTH Smart Sustainable Cities is a new KTH-wide initiative aiming to bundle resources, activities and competence at the intersection of technology, sustainability studies and urban planning. The initiative comes from the KTH Energy Platform and the Centre for Sustainable Communications. Financing is provided by the KTH ICT Platform, the KTH Energy Platform and KTH-Sustainability. The primary goal of KTH Smart Sustainable Cities is to create a contact point at KTH for this rapidly growing field of research.

Coming from Ukraine, I have started up many R&D projects with a network of academic and non-academic partners to support transition of the country towards democracy and energy security.

I am coordinating a Thematic Partnership ReNERGY «Shared visions of sustainable energy systems in cities of the Baltic Sea Region» financed within Baltic Sea Region Programme.

Since 2001, I am a researcher at the Division of Industrial Ecology (IE), Department of Sustainable Development, Environmental Sciences and Engineering (SEED), KTH. I am a co-founder and a leader of a new research group called «Urban Analytics and Transitions» (UrbanT) with two main research areas – Smart Urban Metabolism (SUM) and Transdisciplinary studies for urban transitions (TRUST).

My main research areas are complex system simulation, energy system analysis, participatory backcasting for strategic energy planning, and engineering education in sustainable development. I am a KTH's programme coordinator for the KIC InnoEnergy Master program in Smart Cities.

Olga KORDAS

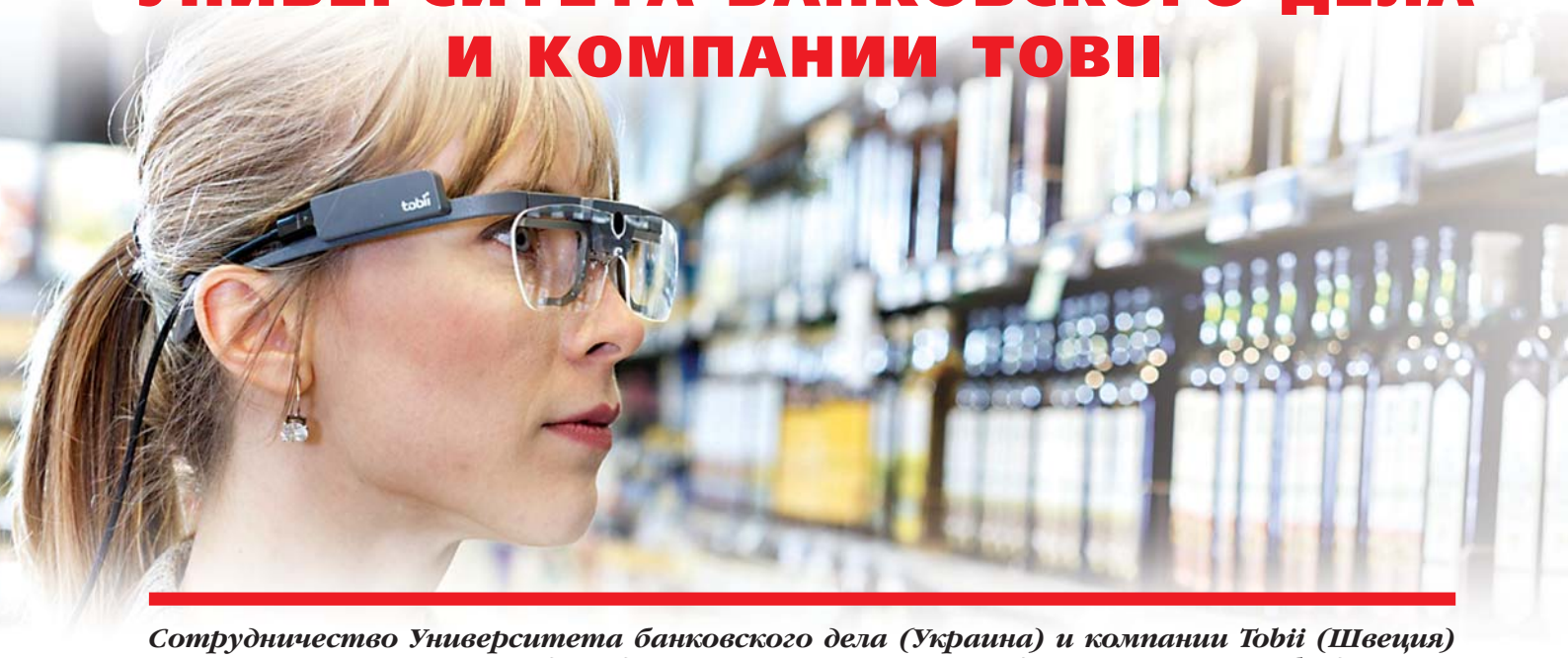
Director of KTH Energy Platform, KTH University, Stockholm, Sweden

Currently I am a Director of KTH Energy Platform, responsible for facilitating interdisciplinary energy research at KTH and enhancing collaboration with funding institutions, industry, local authorities and other societal stakeholders in Sweden and internationally. Since the beginning of 2015, I am KTH's coordinator of STandUP for Energy – a collaboration initiative between Uppsala University, KTH, Swedish University of Agricultural Sciences and Lulea University of Technology, which brings together leading research groups to enable sustainability transition of the energy system.

Together with National Aerospace University «KhAI» KTH has a number of joint EU-funded and Swedish-projects with since 2005, the key ones include Tempus IPMASTER 144628-TEMPUS-2008-SE-JPCR «Intellectual Property Law: New Master Curriculum for the National Consultancy e-Centre on IP management», Tempus Regenlaw 516911-Tempus-2011-DE-JPCR Development of Regional Interdisciplinary Postgraduate Energy and Environmental Studies and Swedish Institute InnoValueNet «Transnational network for facilitating climate of creativity and innovation in Baltic Sea Region». The latter is aimed on establishing international network uniting various stakeholders supporting innovation and entrepreneurship in the Baltic Sea Region, identifying todays challenges and needs for universities and society stakeholders in partner countries in enabling innovations, developing framework for incorporation of entrepreneurial and innovation components into engineering curricula in the partner countries.

KTH VETENSKAP OCH KONST

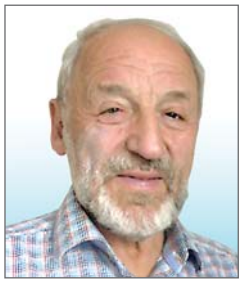
ОПЫТ СОТРУДНИЧЕСТВА УНИВЕРСИТЕТА БАНКОВСКОГО ДЕЛА И КОМПАНИИ TOBII



Сотрудничество Университета банковского дела (Украина) и компании Tobii (Швеция) началось несколько лет назад, когда в Университете созрела идея и появилась необходимость создания лаборатории исследований человеко-машинного взаимодействия.

Александр ГОРДЕЕВ

К.т.н., доцент
Университет банковского дела, Украина



Наум ПУРИЦ

Менеджер по работе с клиентами
компания Tobii

Начнем рассказ с информации об Университете банковского дела и компании Tobii.

УНИВЕРСИТЕТ БАНКОВСКОГО ДЕЛА

Университет банковского дела (г. Киев, Украина) (далее Университет) – государственное высшее ученое заведение IV уровня аккредитации, в котором осуществляется подготовка высококвалифицированных специалистов для финансово-кредитной системы Украины. Университет расположен в городе Киеве и включает структурные подразделения – учебно-научные институты в Черкассах, Львове и Харькове и Институт банковских технологий и бизнеса в Киеве. В университете осуществляется подготовка по следующим специальностям: финансы, банковское дело и страхование, учет и аудит, компьютерные науки и информационные технологии, право.

КОМПАНИЯ TOBII

Компания Tobii – шведская высокотехнологичная компания, которая разрабатывает и продает программное и аппаратное обеспечение для систем слежения и контроля движения глаз чело-

Рис. 1. Очки Tobii glasses

Рис. 2.Eye-tracker Tobii

века. Штаб-квартира находится в городе Стокгольм (Швеция). Структурно компания Tobii состоит из трех подразделений:

- **Tobii Dynavox** – разрабатывает вспомогательные технологии для реализации альтернативных способов коммуникации, включающие специализированное обучение для детей с ограниченными возможностями;
- **Tobii Pro** – разрабатывает исследовательские технологии для изучения поведения человека через движения глаз человека;
- **Tobii Tech** – обеспечивает интеграцию технологий движения глаз человека в продукты других компаний;

Несколько лет назад началось сотрудничество Университета и компании Tobii, когда в Университете созрела идея и появилась необходимость создания лаборатории исследований человеко-машинного взаимодействия. Благодаря поддержки Tobii и проектам Tempus «Knowledge transfer unit – from applied research and technology-entrepreneurial know-how exchange to development of interdisciplinary curricula modules» и «Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» лаборатория была оснащена уникальным высокотехнологичным оборудованием: портативным устройством- eye-tracker (айтрекер) (рис. 2) и мобильным – glasses (очки) (рис. 1).

Рис. 3. В штаб-квартире Tobii с Оскаром Файерсоном и Наумом Пурицем

На следующем этапе сотрудничества после встречи в штаб-квартире Tobii в Стокгольме с вице-президентом Tobii Pro Оскаром Файерсоном и ведущим исследователем компании Наумом Пурицем (рис. 3, 4) был подписан официальный договор о сотрудничестве между Университетом и Tobii и определены дальнейшие направления взаимодействия.

На текущем этапе сотрудничества Университет проводит подготовительные работы для реализации проектов в части исследований человеко-машинного взаимодействия в доменах атомной энергетики и автомобильной безопасности.

Рис. 4. В штаб-квартире Tobii

THE SKYPE STORY

There are very few people among present days web users who have not personally used skype to chat, videocall or have group conference. Not so many have heard how Skype has got its first boost and its later success story.

Juri VAIN

Prof., PhD, Department
of Computer Science
Tallinn University
of Technology
Senior Researcher,
Institute of Cybernetics
Coordinator
of SEREIN project

QUICK LOOK ON FACTS

Skype started from almost nothing in 2003 and created multi-billion Euro value in a short span of time. Apart from creating value and emerging as a strategically important player in the voice and chat connectivity segment of the exploding web business, Skype also won real big time suitors like Microsoft, Google and Facebook.

In its very beginning the Luxembourg-based Skype was owned by an investor group led by Silver Lake and which includes eBay Inc, Joltid Limited and Skype founders Niklas Zennstrom and Janus Friis, the Canada Pension Plan Investment Board and Andreessen Horowitz.

After the formal founding of the company in 2003 by two entrepreneurs, Swedish-born Niklas Zennstrom and Janus Friis from Denmark, Skype made breath taking growth. In three years, Skype had 115 million customers, making it the fastest growing internet community at that time.

Skype has offices in Europe, the US and Asia. It also has offices in San Jose and Brisbane. As of May 2011 Skype already had 911 employees. Its total revenue by the end of same year $859.8 million.

Skype's web services had already 5 years ago an average of 124 million connected users per month. Skype users made 95 billion minutes of voice and video calls in the first half of 2010, approximately 40 percent of which was video.

In 2005, Skype was taken over by the American online auction house eBay for $2.6 billion but eBay sold 70 percent of the stake to Silver Lake Partners.

Earlier 2011, Skype acquired Qik, a mobile video sharing platform. On March 28 same year, Skype accounted for a record 30 million online users simultaneously.

Microsoft CEO Steve Ballmer and Skype CEO Tony Bates jointly announced in May 2011 that the two companies have entered into a deal under which Microsoft will acquire Skype for $8.5 billion.

By year 2014, Skype has reached remarkable 40% of international call market share, and Skype-to-Skype international traffic has gone up to 36% in 2013 to 214 billion minutes.

In 2016 Skype is running practically on all Windows platforms starting from Windows XP to Windows 10 Mobile.

SOFWARE COMES FROM ESTONIA

The hidden side of story is that the Skype software was developed in Estonia by three programmers, Ahti Heinla, Priit Kasesalu and Jaan Tallinn. Skype was their second technological coup, after having launched the software Kazaa in 2001, which grew into a humungous internet exchange site for pictures, songs and videos.

Regardless the change of ownershipin 2011, the skype software development team Skype Estonia has still remained in Tallinn, in the very heart of Tallinn University of Technology (TUT) campus. While started with only three programmers the software development group has grown a multi-national unit with hundreds of employees. Skype is one of the most attractive employer among Estonian IT specialists.

SKYPE AS UNIVERSITY MENTOR

Skype Estonia managing director Andrus Jurg as TUT alumni sees great potential in active collaboration between universities and Skype. Skype supports IT-Akademi programme that was called to life to promote ICT specialities among youth. Andrus Jarg is also one of the initiators of Skype's Foreign Studies' Master's Scholarship Competition launched in 2016.

The Skype foreign studies Master's scholarships are designed to support the Master's studies of two individuals outside of Estonia in the sciences (preferably related to information and communications technology) in 2016, or interdisciplinary studies on condition that one level of higher educa-

tion is completed in the sciences. The aims of the Scholarships are to promote the transfer of knowledge between the sciences and the humanities and the popularisation of ICT specialities and to boost the availability of Master's studies abroad for Master's students from Estonia.

STUDYITIN.ee

Another inititative «Study IT in Estonia Programme» (StudyITin.ee) is managed by the Estonian IT Foundation for Education (HITSA) and sponsored by Skype. The non-profit Foundation seeks to nurture technology talent and supports IT-related educational activities to advance that goal. Though students are expected to cover their tuition and living costs through other sources, the HITSA scholarship fund makes some financial aid available to the brightest students. In combination with university-specific tuition waivers and other aid, the scholarships can make the studies of foreign student in Estonian much more attractive allowign to focus on studies without worring on living.

Each scholarship is worth 8000 euros for the 2016/2017 academic year. The scholarships are designed to cover the cost of tuition fees or other costs related to studies. The period of the scholarships is the 2016/2017 academic year – 10 months. Applications are open to all Estonian citizens and foreigners living in Estonia on the basis of a permanent residence permit who have met the qualifications to enroll in Master's studies.

SKYPE UNIVERSITY HACKATHON 2016

StudyITin.ee in cooperation with Skype is organizing Hackathon for students to create practical IT solutions to any kind of problems that they encounter in real life.This is a 2,5 day event where you can turn your wild idea into something real, get help from Skype engineers, connect with other bright students, build something amazing and have fun!

StudyITin.ee in cooperation with Skype is organizing Hackathon for students to create practical IT solutions to any kind of problems that they encounter in real life.This is a 2,5 day event where you can turn your wild idea into something real, get help from Skype engineers, connect with other bright students. Skype supported activities include:

- Visit to Skype office – hear from Skypers about working in Microsoft.
- Mentors from Skype – more than 10 Skypers will join the Hackathon as mentors and help teams make their wild projects a reality.
- Pitch training – all teams will get pitch training and feedback from pitching experts before the final presentation.
- Cool swag from Skype and StudyITin.ee :-).

CYBER SECURITY – A CHALLENGE FOR WEB SERVICE PROVIDERS

Skype developers have invested years of effort to provide secure and safe services to their customers. IT Academy programme together with Skype is supporting joint Cyber Security and Digital Forensics international study programmes of Tallinn Technical University and Tartu University. Annual summer schools are part of this process to involve leading scientists and practitioners into the education. Practical exercises, moot court, lectures, teamwork with mentors enrich the process with leading edge research and live contacts with professionals all over the world. As for closest event, Cyber Security Summer School 2016 is organised in conjunction with the 2nd Interdisciplinary Cyber Research (ICR) workshop to be held at the Tallinn University of Technology on July 2, 2016. For more information, please visit http://cybercentre.cs.ttu.ee/en/icr2016/

HOW STORIES DRIVE GROWTH

Stanford Business Graduate School in its Marketing and Management course (https://www.gsb.stanford.edu/faculty-research/case-studies/how-stories-drive-growth-skype) presents Skype as one of the learning case. The reason is that Skype has changed our way of thinking and communicating since its appearance. In 2012, Skype needed its customers to transition from using Skype only for important «milestone» life events to using it on regular basis. To advance that goal, Skype created a new marketing strategy, promoting stories about customers using Skype for «everyday moments». Learning about its customers Skype determined how to amplify or market the stories in a way that served its business goals and drive the development of products and services.

Oleg ILLIASHENKO

Assistant lecturer,
Department
of Computer Systems
and Networks at National
Aerospace University «KhAI»
Manager of TEMPUS-funded
projects SEREIN,
CABRIOLET, GREENCO

РЕГІОНАЛЬНІ АСПЕКТИ КООПЕРАЦІЇ ОСВІТИ, НАУКИ ТА БІЗНЕСУ В ІТ-ГАЛУЗІ

Останнім часом в Україні відбувається стійке зростання ваги ІТ-індустрії у загальній структурі фінансових надходжень. Це обумовлено, перш за все, високим рівнем підготовки вітчизняних фахівців з комп'ютерних наук та інформаційних технологій, які посідають одне із провідних місць у світі.

Володимир КАЗИМИР

Проректор з наукової роботи
Професор кафедри інформаційних та комп'ютерных систем
Чернігівський національний технологічний університет
Лауреат Державної премии України в галузі науки і техніки

В то й же час існуюча модель використання цього інтелектуального ресурсу не дозволяє у повній мірі задіяти результати діяльності в ІТ-сфері для розвитку як окремих регіонів, так і країни в цілому. Причина такого стану речей полягає у домінуванні аутсорсингового напрямку діяльності ІТ-компаній, які орієнтовані скоріше на закордонного споживача результатів їх діяльності. Причому ця діяльність, як правило, пов'язана із розробкою окремих частин інформаційно-комп'ютерних систем, що експлуатуються за межами України.

Але якщо виходити із того, що перехід на інвестиційно-інноваційну модель розвитку є одним зі стратегічних пріоритетів економічної політики України, то слід вважати за доцільне переорієнтацію ринку ІТ-послуг з простого виконання завдань окремих клієнтів на створення корисних програмних продуктів, здатних змінювати інфраструктуру споживання. В цьому плані розвиток національної інноваційної системи спирається на інтеграцію зусиль провідних наукових установ, органів державної влади і представників виробництва. На регіональному рівні ці суб'єкти представлені, перш за все, викладачами й науковцями, що працюють в університетах, регіональними адміністраціями та цілою низкою підприємств різних форм власності.

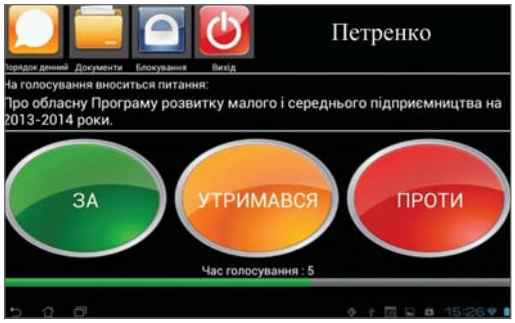
Для прикладу, в північному регіоні Чернігівський національний технологічний університет (ЧНТУ) є найбільшим вищим навчальним закладом, що забезпечує підготовку близько двохсот фахівців ІТ-галузі на рік. В університеті існує три кафедри ІТ-спрямування та ще три кафедри електронного напрямку, які орієнтовані на підготовку спеціалістів з проектування та розробки комп'ютерних систем у різних сферах людської діяльності. Більше половини всіх аспірантів університету, а це майже 50 осіб, навчаються за спеціальностями, пов'язаними із комп'ютерними технологіями. Якщо врахувати, що підготовку цих спеціалістів та науковців здійснюють 7 докторів та 65 кандидатів

наук, то потенціал такого колективу в повній мірі може спрацювати на задоволення потреб не тільки одного регіону. Широкі міжнародні зв'язки, а це перш за все 45 діючих міжнародних договорів про науково-технічне співробітництво, за якими виконується 17 міжнародних проектів, та співпраця у рамках Великої хартії університетів – Magna Chartia Uneversitatum, забезпечують не тільки високий рівень підготовки, але й визнання майстерності виконавців на світовому рівні.

Що стосується потенційних споживачів ІТ-продукції, то тільки у Чернігівському регіоні налічується більше тисячі підприємств, які представляють промисловий та аграрний сектори економіки. Окрім них у використанні новітніх ІТ-розробок зацікавлені органи регіонального та місцевого самоврядування, чисельні державні установи, заклади охорони здоров'я та освіти. Таким чином, на даний момент існує проблема ефективного використання значного інтелектуального потенціалу технологічного університету для потреб регіону, яка може бути вирішена через впровадження інноваційних розробок в ІТ-сфері.

Вирішення даної проблеми потребує застосування нових підходів як у технологічному, так і фінансово-економічному плані, які будуть здатні мобілізувати зусилля ІТ-спеціалістів та досягти поставленої мети. Зрозуміло, що з точки зору технологій аутсорсингова модель взаємодії науки та бізнесу не залишає шансів бути успішною в цьому плані. Тому на зміну їй повинна прийти більш продуктивно спрямована модель R&D (Research and Development). В загальному розумінні модель R&D може бути застосована за двома формами, а саме: розробка нових ІТ-продуктів та генерація нових знань, що можуть бути використанні у подальшому для створення тих же самих продуктів чи забезпечення нових процесів та послуг. Обидві ці форми моделі R&D мають право на життя і можуть бути більш чи менш корисними в залежності від негайних бізнес-інтересів та потреб замовника та споживача.

Як приклади успішного застосування вказаних форм моделі R&D у ЧНТУ можна навести цілу низку виконаних



ІТ-проектів. Перш за все, це стосується створення вітчизняного UA Криптофону – пристрою для забезпечення шифрованого зв'язку високої стійкості при використанні стандартних мобільних мереж. До основних переваг пристрою відносяться: апаратне та програмне забезпечення власної розробки, робота у двох режимах (звичайного та захищеного зв'язку), стандартний інтерфейс користувача мобільного телефону, захист голосових переговорів та SMS повідомлень, висока якість розмови у захищеному режимі, автоматичне розпізнання режиму вхідного дзвінку, посесійна зміна ключів криптування та автоматичний контроль їх наявності. Розробка пройшла всі види випробувань та сертифікацію, захищена патентом.

На основі попередньої технології була розроблена система захисту інформації в мережах IP-телефонії та цифрового радіозв'язку із забезпеченням завадозахищеності телекомунікаційних систем. Система включає апаратно-програмні засоби завадостійкого кодування інформації в умовах впливу навмисних завад та забезпечує проведення захищених голосових конференцій у IP-мережі та мережах радіозв'язку. Система пройшла випробування та захищена патентом.

Для аграрного сектору пропонується система автоматизації управління процесами рослинництва, яка забезпечує планування та оперативне управління роботами агропідприємства по вирощуванню рослин. Принцип роботи системи грунтується на використанні вбудованих математичних моделей, що враховують невизначеності, та геоінформаційної системи. Система має логістичну підсистему, що забезпечує формування та контроль виконавчого плану у реальному часі.

У сфері охорони здоров'я розроблена мобільна інформаційна система кардіодіагностики. Система забезпечує аналіз та відображення електрокардіограм, що зберігаються у національній базі даних МЕДГРІД з можливістю віддаленого доступу до бази даних МЕДГРІД з мобільного пристрою, ідентифікацією ЕКГ по QR-коду, експрес-аналіз отриманих ЕКГ, відображення ЕКГ на дисплеї мобільного пристрою. Розробка завершена та впроваджена. Портативний кардіограф-енцефалограф забезпечує моніторинг стану серцевого ритму людини з використанням 8-ми незалежних каналів вимірювання, має малі габарити 120х60х15мм та масу 250г, з'єднання з смартфоном або планшетом для відображення сигналів, швидкісні інтерфейси USB 2.0, CAN 2.0, Bluetooth, Li-Ion акумулятор з автоматичною підзарядкою від ПК.

Комп'ютерна програма «Єдине інформаційне вікно» представляє собою інтернет-орієнтовану програмну систему для розробки та підтримки функціонування єдиних інформаційних вікон з надання адміністративних послуг. Програма має вбудовані моделі процесів документообігу, які легко налаштовуються під вимоги організації, інтуітивнозрозумілий інтерфейс, електронний підпис документів.

Найбільш апробованою серед IT-розробок фахівців є ЧНТУ електрона система голосування Mobile-RADA, яка вже більше 4 років успішно працює у Чернігівській обласній раді. Система забезпечує автоматизацію роботи депутатів під час проведення сесій за допомогою планшетного комп'ютера, підключеного до захищеної бездротової мережі, виключає необхідність перебудови сесійних залів і забезпечує мобільність й зручність у роботі депутатів рад за рахунок використання електронного документообігу і електронної панелі голосування.

Безумовно, всі наведені IT-проекти є високотехнологічними та мають інноваційну спрямованість. Але ефективність використанням моделі R&D стримується існуючими фінансовими умовами, які не сприяють створенню наукоємних IT-продуктів. Тому невід'ємною частиною технологічного аспекту повинна стати нова економічна модель.

Світовий досвід показує, що при правильному використанні вільних економічних зон (ВЕЗ) як форми правового регулювання діяльності підприємств, вони можуть комплексно розв'язувати проблеми розвитку окремих регіонів на основі інноваційного процесу з урахуванням економічної політики держави по структурній перебудові економіки. Яскравим прикладом в цьому є Китай. Фактично, створення особливих економічних зон дозволило використовувати відкритість економіки Китаю для реалізації його промислової політики. Аналіз китайського досвіду показує, що багато в чому це стало можливим завдяки використанню вищих навчальних закладів як бази для створення ВЕЗ. Переваги ВЕЗ саме при університетах не обмежуються тільки наявністю висококваліфікованих кадрів, але й новими суспільними формами, головна мета яких – сприяння зв'язку науки з виробництвом і економікою.

Для України сьогодні такий досвід Китаю може стати багато в чому до снаги. По-перше, завдяки політиці, що проводить Міністерство освіти і науки в напрямку укрупнення державних університетів, вони стають дійсно інтелектуальними центрами регіонів. По-друге, такі університети залишаються інституціями, через які може бути відпрацьований дійсний механізм ефективного державного регулювання розвитком ВЕЗ. По-третє, університети є провідниками інноваційного розвитку, оскільки можуть забезпечити підприємства необхідними кадровими ресурсами.

Не можна говорити, що створення ВЕЗ при університетах є дорогою з одностороннім рухом – від університету до регіону. Завдяки ВЕЗ сам університет отримує колосальні можливості для свого розвитку, одночасно не стаючи тягарем для держави. Це стосується і розширення матеріально-технічної бази, і практичного спрямування підготовки студентів, і працевлаштування випускників в Україні, і стимулювання роботи викладачів. То ж, окрім чисто економічного впливу, концентрація ВЕЗ навколо університетів здатна вирішувати і цілий ряд соціальних проблем регіонів, стаючи дійсно локомотивом їх сталого розвитку.

КАК СТАРТОВАТЬ В R&D

- Как учить R&D?
- Экосистема для стартапов: акцент на R&D
- Как «запускать» технологический венчур?

MODIFICATION OF UNIVERSITY CURRICULA ACCORDING TO R&D IN INFORMATION SCIENCE AND TECHNOLOGY: AMERICAN AND UKRAINIAN EXPERIENCES

Prof. Dr. Yuriy KONDRATENKO

Petro Mohyla Black Sea State University (Ukraine)

Prof. Dr. Dan SIMON

Washkewicz College of Engineering at Cleveland State University (USA)

The problem discussed in this paper is the need to prepare university graduates according to modern developments in information science and technology, and according to new research and development (R&D) achievements in the corresponding fields of knowledge. The solution to this problem requires the modification of university curricula for both undergraduate and graduate students based on advanced international and cutting-edge research results. The discussion is based on experiences and examples from the Washkewicz College of Engineering at Cleveland State University (CSU) in Cleveland, Ohio, USA; and Petro Mohyla Black Sea State University (PMBSSU) in Mykolaiv, Ukraine.

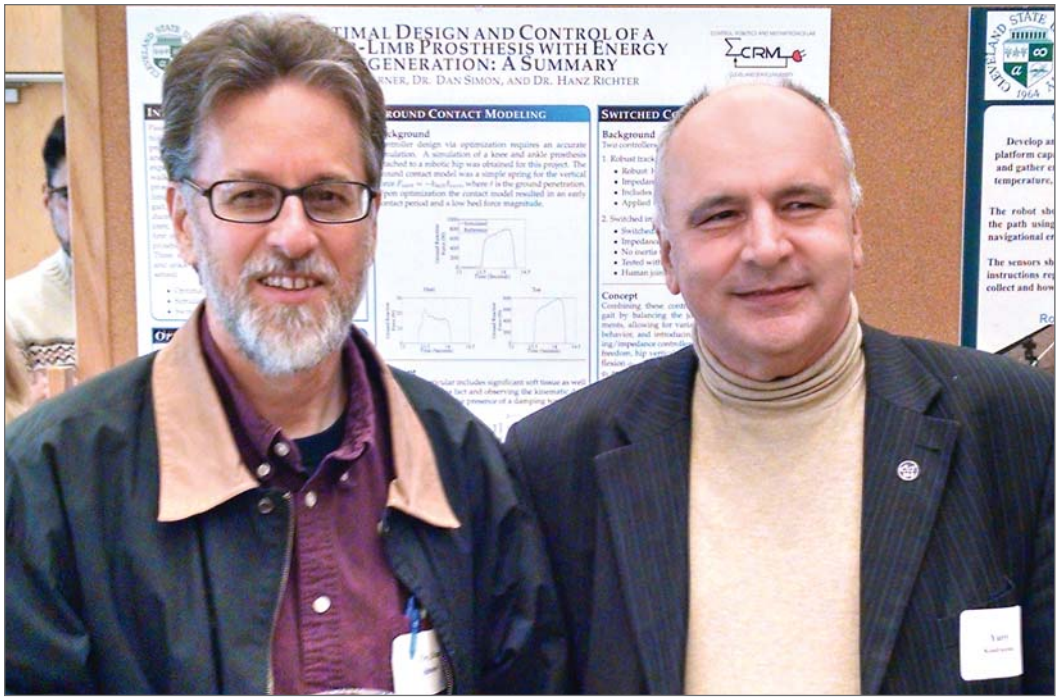
Many countries are reforming their science and technology systems to include recent advanced R&D results in higher education. All of these countries have to solve the same problem: how to create university curricula while providing a balance between theory and practice, and how to flexibly modify such curricula based on new R&D achievements and developments. This modification must take into account the dynamics of economic development, regional and national markets and priorities, the increasing technological level of engineering and scientific processes, the complexity of market relations and the labor market, and the globalization and internationalization of society and educational systems.

The need for curriculum modification according to current R&D achievements and activities is common among various countries, but with national differences in some aspects, so it is important to share best practices at the international level. We consider three main approaches for the modification of university curricula based on R&D achievements in information science and technology.

- **First**, university curricula can be modified by introducing new fundamental and elective courses, or by modifying the content of existing courses, while taking into account that the current educational system in many countries allows for elective courses. For example, the Master of Science in Electrical Engineering program at CSU

includes 14 elective courses for the Computer Systems specialization, including Embedded Systems, Software Engineering, Modern Digital Design, Rapid Digital System Prototyping, Formal Methods in Software Engineering, Software Quality Assurance, Software Testing, Software Design & Architecture, High Performance Computer Architecture, Distributed Computing Systems, Computer Networks II, Parallel Processing Systems, Mobile Computing, and Secure and Dependable Computing. All of these elective courses can be modified in a timely manner by tracking and incorporating new developments in the following areas: computer-aided design software that enables new capabilities in the design of various devices, machines, ships, etc.; information technology approaches for industrial and domestic applications for teaching more efficiently, and for monitoring, controlling, and testing student knowledge; internet-based methods for applying current international standards to education; and many others.

- **Second**, special attention should be paid to research-based education by incorporating new R&D achievements and advanced software in undergraduate, graduate, and doctoral student research (course work, diploma projects, and theses). This activity should be pursued within the framework of government priorities. For example, PMBSSU has received research grants from the European Commission for TEMPUS, including the project «Model-Oriented Approach and Intelligent Knowledge-Based System for Evolvable Academia-Industry Cooperation in Electronics and Computer Engineering». CSU has received research grants from the US National Science Foundation (NSF), Cleveland Clinic, Innovative Developments, Ford Motor Company, American Diabetes Association, Electronics and Telecommunications Research Institute, and others. CSU's research projects include «Optimal prosthesis design with energy regeneration» (1.5M USD), «The game changer: A new model for password security» ($200,000), «Acquisition of a 4G/LTE wireless communications test set» ($252,000), «A spiral computer engineering lab framework» ($245,000), and others, all funded by the US NSF. Student participation in all aspects of these research projects is significant for increasing the level of their qualifications upon graduation. CSU students conduct research using the following software: Altera Quartus II 10.1 SP1, Altera Quartus II 13.1, Cisco Packet Tracer, Oracle VM VirtualBox, Microsoft SQL Server 2008, Microsoft Visual Studio 2010, Microsoft Office 2010, Orcad family Release 9.2 lite Edition, ORCAD 16.5 lite, Python 2.7.5, MATLAB R2013b, dSPACE Control Desk 5.1, ModelSim SE 10.0a, Precision Synthesis 2010 a.218,



Prof. Dr. Dan SIMON (left), Prof. Dr. Yuriy KONDRATENKO (right)

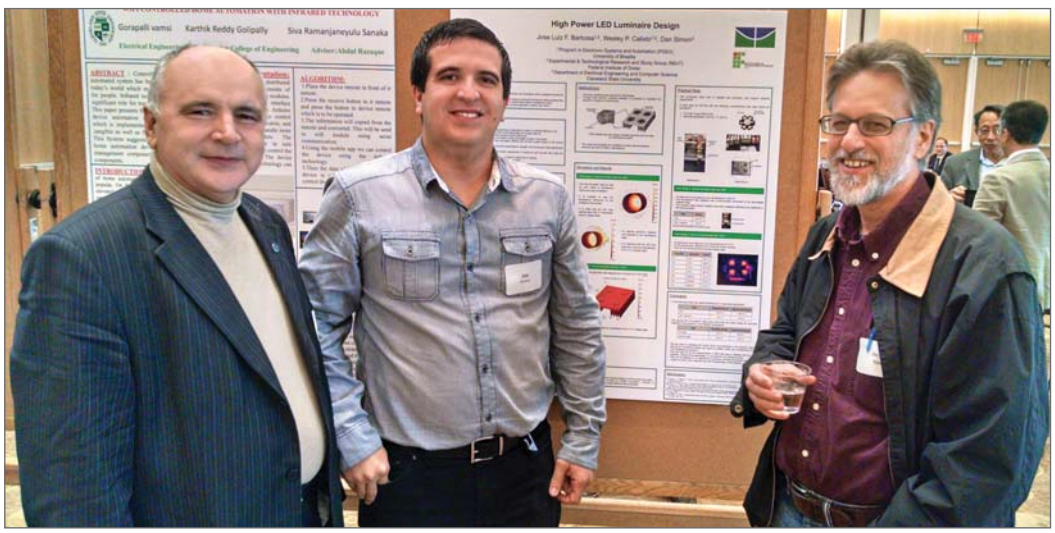
SystemView V6.0, and Agilent Data Capture Application, among others. PMBSSU students conduct research using the following software: Visual Studio, MS SQL Server, MS Windows Server, MS Windows 7, MS Access, MS Visio, MS Project, Free Ware, Moodle, Libre Office, Eclipse, NetBeans IDE, Ubuntu, FreeBSD, Apache, Qt, OmegaT, VirtualBox, Python, Java, JavaFX, C/C++, PHP, JavaScript, and HTML5, among others.

• **Third**, education should include academic or academic-industry consortia. Academic consortia allow cross-registration among cooperating universities. The term «cross registration» means that students have the possibility for simultaneous study at their home universities and elective courses at other universities (members of academic consortia), depending on student interests, abilities, and aspirations. Cooperation between universities and advanced information technology (IT) companies is a powerful mechanism for knowledge transfer within the framework of lectures by IT company representatives at the university, familiarization of students with new IT company software, student internships (Global Logic, NASA Glenn Research Center, General Electric, etc.), joint research projects, students certifications, the incorporation of industry research results in university curricula, and the creation of student start-up and spin-off companies.

PMBSSU students who have been involved in research-based and academic-industry-based education have been repeat winners in the Aldec, Inc. (USA) Olympiad on C++, VHDL and Verilog. A CSU student team took first place at an international student design competition sponsored by the American Institute of Aeronautics and Astronautics. These are two of many cases of industry-based and academia-based research and education. University-IT company cooperation in research and education opens a wide spectrum of opportunities for university student careers and employment. Some examples include: (a) CSU graduates work in US companies and industrial corporations such as Rockwell Automation, Phillips, Foundation Software, Winncom Technologies, UTC Aerospace Systems, Swagelok Company, RoviSys, American Railways, United States Postal Service, and others; (b) PMBSSU graduates work in Canada, France, Germany, Great Britain, Latvia, Netherlands, Norway, Poland, UAE, USA, and Ukraine, including companies such as Camo-IT, Ciklum, eBay, EPAM Systems, GeeksForLess, GlobalLogic, HostingMaks, Linkedln, Luxof, Microsoft Research, MobiDev, NetCracker, Oracle, TemplateMonster, and others.

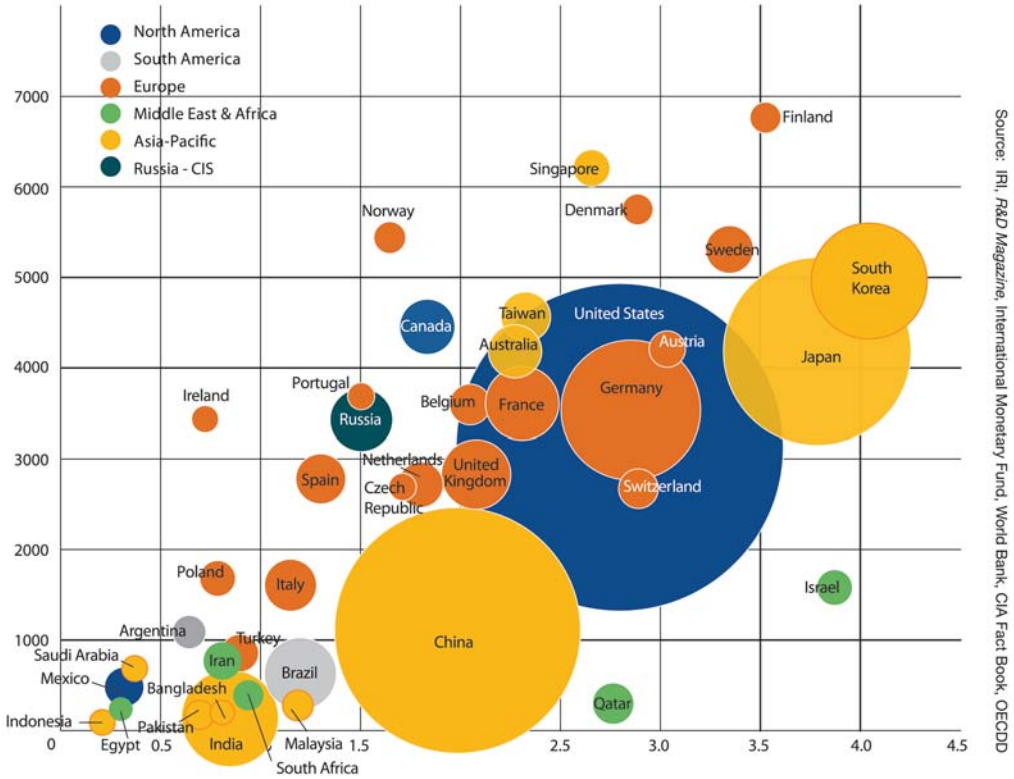
The three approaches summarized above modified elective courses, research-based education, and academia-industry education are based on R&D achievements in information science and technology. If they are successfully introduced in higher education today, then tomorrow's IT-based companies, government research agencies, and national laboratories will obtain the high-quality graduates that they need. New R&D achievements in information technology require continuous monitoring by educators, and implementation in education.

• **Acknowledgements**. The authors gratefully thank the Fulbright Program (USA) for providing the possibility for joint research in the USA by supporting Prof. Y. P. Kondratenko with a Fulbright scholarship.



2016 GLOBAL R&D FUNDIDNG FORECAST

(Continuation from the page 2)



Source: IRI, *R&D Magazine*, International Monetary Fund, World Bank, CIA Fact Book, OECDD

Size of the circles reflects the relative amount of annual R&D spending by the indicated country. Note the regional grouping of countries by the color of the balls.

** Source: R&D Magazine, Industrial Research Institute and Research-Technology Management. http://www.rdmag.com/topics/global-r-d-funding-forecast

КООПЕРАЦИЯ УНИВЕРСИТЕТА И ИНДУСТРИИ – СТРАТЕГИЯ WIN-WIN

Всем известно очарование слова – dessert. Но достаточно потерять только одну букву и из симпатичного сладкого блюда получиться desert – пустыня. Внимание к деталям важно не только в написании слов, а и в их имплиментации – в подходах и реализации этих подходов.

Уже два года на базе Одесского национального политехнического университета (ОНПУ) работает украинско – канадско-немецкая международная Стартап Школа. В основу концепции Школы положено несколько довольно очевидных идей. Реализация проектов в Стартап Школе становится возможной, благодаря кооперации вуза – как базовой организации, его иностранных партнеров, специалистов из индустрии, которые выполняют функции менторов и представителей бизнеса.

Михаил ЛОБАЧЕВ

К.т.н., профессор, PMP
Директор международной Стартап Школы
Одесский национальный политехнический университет

Хочется заметить, что без участия университетской бюрократии (в хорошем смысле этого слова) успешная работа над таким проектом крайне затруднительна. От степени ее вовлеченности во многом зависит окончательный результат. Говоря языком проектного менеджмента, она – один из главных стейкхолдеров.

Ниже приведен рисунок, который мы условно назвали Start-Up School Eco-system (рис. 1).

В нашем случае идею проекта предоставляет кто-либо из наших канадских партнеров из индустрии или из числа немецких коллег. Они же выполняют функции технических консультантов.

Проект, как правило, находится в струе какого-либо технологического тренда, но по каким-то причинам компания не готова потратить на его имплементацию значительные средства. Однако сама идея представляет для компании интерес. В рамках стартап школы такой проект может быть реализован до уровня получения прототипа. Таким образом, реализуется, так сказать, «Proof of concept». В дальнейшем, в зависимости от полученных результатов, может приниматься решение о продолжении работ либо проект так и останется оригинальной студенческой разработкой. Та-

ким образом, Стартап Школа может убить при хорошем раскладе сразу двух зайцев.

Если разработка представляет коммерческий интерес, она может перейти в рязряд стартапов. Если же нет, в активе у студентов появляется научная публикация по данной теме, хорошие технические навыки в области данного технологичекого тренда, опыт работы в международной команде, соответствующие связи в индустрии и академических кругах, а также опыт в работе над реальным проектом, включая его бизнес-составляющую.

Распределение ролей происходит приблизительно так, как показано на рисунке 1. По окончании проекта студенты, в известной степени, уже являются экспертами в области разрабатываемого концепта.

На сегодняшний день работы в школе ведутся по различным направлениям. Это как интернет-приложения, так и комплексные программно-аппаратные решения, включая направление так называемых носимых устройств (wearable devices).

Приходится заметить, что построение специализированных систем на базе микроконтроллеров представляет определенную сложность, как для украинских, так и для немецких студентов. Заметно, что в последнее время акцент в обучении явно смещался в область программирования различных приложений.

Однако последние новости от компании Intel, которая обьявила о значительном сокращении своих сотрудников и смещении акцента в разработках в область специализированных устройств, говорит о сомнительности такого подхода на компьютерных факультетах и необходимости корректировки в программах.

В настоящее время мы работаем над программой двойных магистерских дипломов с университетом Аугсбурга, Германия. Для получения такого двойного диплома студенты должны набрать определенное количество кредитов в партнерских университетах. Значительная часть из них – это совместная работа над проектом в Стартап Школе. При этом подразумевается, что работа будет происходить в интернациональных командах. Использование R&D в качестве одного из компонентов обучения становится все более популярным.

Например, североамериканские вузы давно практикуют в качестве финального аккорда в обучении бакалавров большой десятикредитный проект, который длится почти весь четвертый курс (хотя понятие курса весьма условно в кредитно-модульной системе) и подразумевает тесную кооперацию с индустрией, так как чистые теоретики уже давно не слишком востребованы, особенно в инженерии.

Наш опыт показал, что в той или иной степени большинство прогрессивных университетов стараются использовать R&D как часть системы подготовки инженерных специалистов.

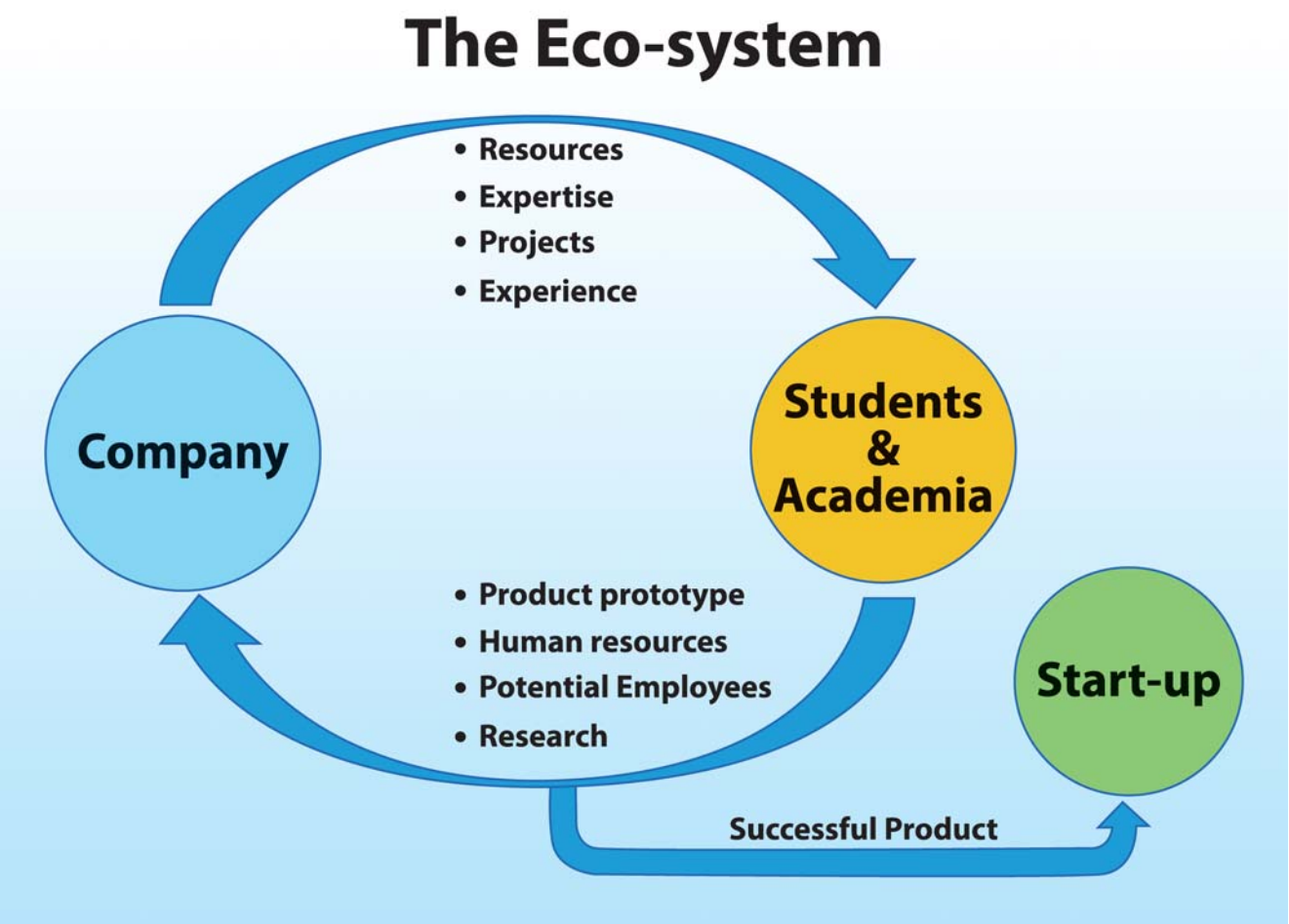
Разница между североамериканскими, европейскими и украинскими университетами, на наш вигляд, состоит лишь в возможностях (материальных и интеллектуальных), традициях, сложившихся подходах и способностях воспринимать инновации.

Светлана АНТОЩУК

Д.т.н., профессор
Директор Института компьютерных систем
Одесский национальный политехнический университет

РИСУНОК 1

START-UP SCHOOL ECO-SYSTEM



Возможно это прозвучит странно, но университеты – это довольно забюрократизированные структуры, где инновации воспринимаются сложно. В этом плане бизнес является более гибким и восприимчивым ко всему новому.

В университете Аугсбурга есть магистерская программа «Master of Research», концепция которой схожа с концепцией, реализуемой в нашей Стартап Школе. С той лишь разницей, что в Стартап Школе в последовательность: Обучение (Studying) – R&D (Research and Development) добавляется еще одна составляющая – Management.

В условиях современного рынка, где молодые специалисты имеют большие проблемы с трудоустройством, важно не только иметь релевантные знания, уметь их применять на практике, но еще и уметь ориентироваться в этом рынке, что добавляет инженерам новые, не свойственные им функции.

В силу этого предполагается в качестве развития Стартап Школы ОНПУ и немецкой программы «Master of Research» создать программу, которая условно будет называться EMBA – MBA для инженеров, где, кроме обучения и разработки реальных продуктов для индустрии, студенты получат довольно специфические знания из области проектного менеджмента, а также работы с заказчиками инженерного продукта и инвесторами.

А чтобы было понятно, что может получиться в результате работы Стартап Школы, прежлагаем рассмотреть пример проекта, который, скорее, ближе к области R&D, чем к стартапам, основной задачей которого было научить студентов разрабатывать приложения и оборудование для носимых устройств, а также научиться работать с RTOS QNX.

ПРОЕКТ

«ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРЕДАЧИ ТЕЛЕМЕТРИЧЕСКИХ ДАННЫХ НА НОСИМОЕ УСТРОЙСТВО»

Современное обучение в университетах бывает недостаточным для полной подготовки студентов к работе в сфере своей специализации. Для расширения кругозора, ознакомления с новейшими технологиями вводятся факультативные занятия и проводятся различные проекты вне учебы. В данном кейсе показан пример разработки, выполненной студентами Стартап Школы.

В рамках проекта совместно с канадскими партнерами была разработана информационная система для передачи телеметрических данных на носимое устройство под управлением RTOS QNX. На рис.1 показано как универсальное устройство передает координаты GPS на Pebble Watch.

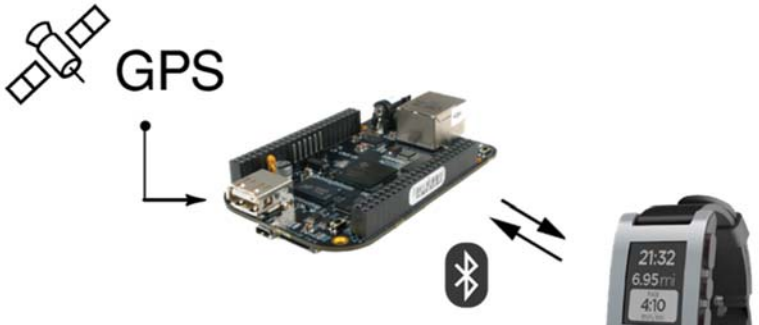


Рис. 1. Передача координат GPS на Pebble Watch.

Основной задачей проекта было создать и протестировать универсальный беспроводной канал связи между устройствами с различной архитектурой и различными операционными системами. При этом разработка должна была проводиться в системе реального времени для своевременной обработки поступающих данных и актуальности переданных данных.

Рис. 2. Функциональная схема универсального Gateway.

Наиболее трудные моменты, которые возникли у студентов в процессе разработки, были связаны с работой на различных, ранее не известных платформах - RTOS QNX и отсутствием некоторых необходимых готовых драйверов для работы с подключаемыми устройствами.

Рис. 3. Процесс обмена данными.

После анализа функционала «посредника» Gateway (рис. 2) данные поступают от источника и передаются в обработчик через USB COM-порт. Эти данные будут обработаны, где из них будет выделена строка с необходимой информацией. Далее они будут разложены в поля структуры для комфортной работы с ними.

Модуль GPS имеет интерфейс USB. Модуль генерирует массив информацию о его местонахождении в формате NMEA-0183 («National Marine Electronics Association»).

Для разбора и обработки была выбрана строка GPRMC, где указываются источник, время по Всемирному координированию времени, статус, широта (северная, южная), долгота (восточная, западная), горизонтальная составляющая скорости, путевой угол, дата и контрольная сумма.

В ходе работы был изучен протокол обмена данными с Pebble (рис. 3) и разработана библиотека для работы с часами, которая позволяет обмениваться данными между Beagle Bone и Pebble. Так как часы Pebble работают со специфическим протоколом обмена данных, была изучена и разработана структура пакета.

В зависимости от необходимости, устройство может использоваться яхтсменами для оперативного получения текущей информации на носимое устройство, в промышленности, в медицине для связи с диагностическим оборудованием, в системе служб по чрезвычайным ситуациям.

Кстати, данный проект как раз и занял первое место в конкурсе студенческих проектов, который проходил под эгидой Государственной службы по чрезвычайным ситуациям. ■

THINKING «SILICON VALLEY»: CASE STUDY AND LESSONS LEARNT

During October – November 2015 I had a chance to participate at the new initiative of Silicon Valley tech and academic community – Technology Venture Launch Program (TVLP), hosted in Menlo Park, California. Silicon Valley (SV) TVLP positioning itself as «a 20-day immersion program on technology venture creation that provides state-of-the-art training along with valuable networking opportunities with Silicon Valley investors, entrepreneurs and service providers». It primarily intended for those seeking to acquire a Silicon Valley mindset as they prepare to start a technology venture. It's suitable for scientists, young entrepreneurs, or managers as well as for those interesting in being directly exposed to the Silicon Valley environment. Our group (autumn intake 2015) included 9 participants from UK, Italy, Germany, France, USA and the only one participant from Ukraine who wants to share some program insights by writing this paper ☺.

The three-week program is made up of three parts: Instructor-led courses, group work led by individual mentors, site visits and networking events.

Within the teaching module TVLP academic staff provided us business fundamentals necessary to successfully launch a technology venture – either for PortFoleo (marketplace for prominent architects and industrial designers) or LabCollector (collaborative system for academic and industry Lab R&D to manage all kind of assets and biological data). The key academic advantage was that all classes were taught by a faculty who are Silicon Valley university professors. For example Marketing was taught by Dr. Juan Montermosso, who is a professor at Santa Clara University and

teaches competitive marketing strategy in the MBA program, ranked among the top 20 part-time programs in the U.S. He holds a B.S. in Engineering and Applied Science from Yale University, an M.S. in Applied Math and Computer Science from Harvard University, and a Doctorate in Business Administration from the Harvard Business School.

Curriculum delivered to our group included set of classes covering both start-up fundamentals and functional skills: team building (leadership techniques, choosing cofounders, setting up incentives etc.), strategic positioning (market research, product management, value proposition, revenue models etc.), business development (sales, partnership, scaling of venture) and startup finances (bootstrapping, fundraising, pitch decks). The only problem was that all participants have high but different initial background and prerequisites – MA in architecture, MSc in international economics, MBA, 2 PhDs in math and computer science – which lead sometimes to difficulties in understanding high-level theory in financials and business development.

The objective of the second module – group work and mentoring – was to develop a pitch – a short but efficient presentation of business idea for investors and partners using student's own startup ideas. A set of experienced professors (one in marketing and sales, second in business development, third one in public speaking) have provided students with the essential elements on how to create and validate a consistent pitch deck in line the formal chain: «customer problem – my solution – market opportunity – competition – team – revenue model – go-to-market strategy – capital seeking – financials – exit strategy». During the second period of the module we have applied the acquired methodology to our own venture idea. In my case it was the developing and fine tuning of the pitch deck for my previous startup – Tornado gloves by Global DJ which help DJ, vocalists and musicians to create amazing live shows by gestures only.

The last but definitely not the least part of TVLP program was devoted to the essential part of Silicon Value culture – intensive networking sessions and on-site visits. Our group (tired from intensive everyday teaching and training sessions but very well motivated to learn well known cases and success stories) had a chance to meet some of the experienced SV investors including business angels and venture capitalists like Canaan partners, Bosch Venture Capital, Lux Capital, Keiretsu forum. On same day we have attended the special private events in Churchill Club "The Intel Trinity" and SV forum, listening to the public speeches of Cisco VP and Symantec CEO. The third group of site visits was aimed to get us acquainted with latest R&D developments and corporate culture in Google, Apple, LinkedIn and Intel corporations, as well as Stanford university (which has the biggest number of Nobel Prize Laureates, operates enormous 62 bln annual budget and acts as «motherland» for the significant part of successful star-

Artem BOYARCHUK

Dr., Senior lecturer
Department of Computer Systems and Networks
National Aerospace University «KhAI»,
Kharkiv, Ukraine

tups in Silicon Valley and worldwide): the limitations of the current paper does not allow to share all knowledge and insights of the visited giants. I'm happy to briefly mention only two of them – lectures of two «iconic faces» of contemporary Silicon Valley: Alberto Savoia and Guy Kawasaki.

Alberto Savoia, former Chief Technology Officer in Sun Microsystems and ex-director of Google AdWords, now acts as an expert, coach, author and speaker on the topic of high-yield innovation through experimentation. Today he is focused on a tough problem aimed on helping companies make sure that they are building the right things using the concept of «pretotyping». That means the set of structured techniques on how to test the viability and market potential of startup idea on its very initial phase having invested slight costs in marketing and zero costs in production. Funny but cool fake ideas like «outdated sushi» and «beer for dogs» were taken by Alberto as an example to illustrate the implementation for pretotyping methodology.

The second outstanding event was the lecture «The Art of the Start 2.0» by Guy Kawasaki, one of the most successful keynote speakers in the world. His clients include Nike, Apple, Gartner, Microsoft, Shire, Google, Clorox, and Genentech. He covers the topics of innovation, sales, persuasion, and social media. Being today a chief of marketing in Canva (online graphic-design company from Australia) and brand ambassador of Mercedes Benz he is world-wide known person as Apple chief evangelist – a person who introduced together with Steve Jobs the Apple philosophy of «the best tech product ever».

The program was finalized by graduation party with presentation of selected students' pitch decks for invited serial entrepreneurs and angel investors and an informal dinner with them.

From my personal feeling the most important lessons learnt from the program and networking sessions which definitely worth of costs spent include both formal and informal knowledge: advantages and potential troubles of the current «hot» subject areas of startup developments (Artificial Intelligence; Virtual/Augmented Reality; Shared Economy; Drones and Robotics); opinions about «Silicon Valley bubble»; tips and tricks on composing the founders' team and planning the business model; practical cases and advices on how to plan the fundraising in order to avoid frequent mistakes; differences between US and European startup ecosystems, and how to turn them into founder's opportunities.

НАУКА, КАДРЫ ДЛЯ R&D

- Взгляд ИТ-аспиранта
- Что и как делать ИТ-дизайнерам в науке?
- Трансдисциплинарность – синергия для R&D?

О ЧЕМ ГОВОРЯТ PHD СТУДЕНТЫ В ОБЛАСТИ КОМПЬЮТЕРНЫХ НАУК...

Обсуждая развитие кооперации науки, образования и ИТ-индустрии в Украине, а также перспективы инновационного Research and Development (R&D), мы не должны забывать о главных его участниках, а именно о студентах, аспирантах и докторантах, которые часто являются единственным связующим звеном между университетом и компанией, и действительно выполняют как исследования, так и разработки. Как минимум с их позиции отчетливо видны практические проблемы в отношениях между наукой и индустрией, понимание которых необходимо для поиска решений. Еще недавно, будучи студентом ведущего украинского университета (ХАИ), участником олимпиад по программированию, стажером большой аутсорсинговой ИТ-компании и техническим директором небольшой стартап-компании, я лично испытал затруднения, с которыми сталкиваются студенты в научной работе и коммерческих разработках, несмотря на поддержку кафедры.

Интересным, но не удивительным фактом является то, что большая часть этих затруднений исчезла сама собой, когда я стал PhD студентом в нью-йоркском вузе. Все начинается с того, что сама граница между наукой и бизнесом в западных вузах размыта, ведь компании активно сотрудничают с исследовательскими лабораториями, выдают гранты, предлагают исследовательские R&D стажировки для PhD студентов, участвуют в научных конференциях и сами активно публикуют научные статьи! Существует и много других прогрессивных примеров, которые я постараюсь кратко описать. Надеюсь, что в ближайшем будущем украинские вузы и компании смогут перенять и улучшить данные полезные практики. Изложенные ниже выводы основаны на моем личном опыте и наблюдениях, но я постарался уловить популярные тренды. Итак, о чем же говорят студенты (они же – молодые ИТ-специалисты) в Украине?..

ЗАЧЕМ ПОСТУПАТЬ В АСПИРАНТУРУ?

Многим украинским студентам тяжело ответить на данный вопрос, ведь на момент получения диплома специалиста или магистра они уже работают в локальных аутсорсинговых компаниях и имеют перспективу хорошо оплачиваемой работы. Действительно, зачастую главным фактором в принятии такого решения является экономический. В случае западных университетов ситуация аналогична: зарплата PhD студента намного меньше, чем доходы в ИТ-индустрии. Тем не менее получение степени PhD является довольно популярным желанием и в любом случае считается престижным выбором. Почему?

- **Во-первых**, ценность степени PhD прозрачна. Существует большой запрос на исследователей в области компьютерных наук, и известно, что, работая в X Research, можно добиться больших карьерных успехов, чем работая программистом в X. К сожалению, на данный момент в Украине мало компаний по достоинству оценивают докторскую степень, в отличие от опыта кодинга, да и мало компаний занимаются изобретением программных продуктов и технологий. Это объясняется тем, что украинская ИТ-индустрия еще находится на этапе развития, но сдвиг от аутсорсинга в сторону R&D нужно ускорять, и отдельные успешные примеры существуют.
- **Во-вторых**, степень PhD, полученная в западном вузе, часто авторитетнее, и мало у кого из работодателей возникнет вопрос о квалификации молодого доктора для выполнения R&D. Здесь можно упереться во внешние экономические и политические преграды, а можно подумать, как повысить рейтинг и авторитет наших университетов. Вариантов много, включая более практическую, бизнес-ориентированную подготовку студентов и дальнейшую результативную интеграцию в международную научную кооперацию.

• **В-третьих**, западные компании практикуют специальные стажировки для PhD студентов, являющиеся обоюдно полезными, поскольку во время стажировки студенты помогают в исследовательской деятельности для создания инноваций, а сами получают финансовую поддержку. Кроме того, продолжительность стажировки лимитирована, что не отвлекает студентов от завершения учебы, а если они понравились компании, их будут ждать на стажировки каждое лето.

ЗАЧЕМ ПИСАТЬ СТАТЬИ?

Отсутствие мотивации в данном вопросе не позволяет студентам заинтересоваться научной работой, а аспирантам – продуктивно работать во время обучения в аспирантуре. Особенно, когда есть выбор: выполнить проект на работе, который, кроме зарплаты, принесет ценную строчку в резюме, или потратить время на написание научного текста. В чем же проблема?

Часто можно услышать жалобы наподобие «мое исследование никому не нужно», «никто не будет читать мою статью», «публикация требует соблюдения многих формальностей»... К сожалению, доля правды есть в каждой из них. И опять-таки мой опыт в этой сфере полностью изменился, когда я начал публиковать статьи в США и Европе.

• **Во-первых**, первоначальная цель – это всегда самые популярные конференции, в которых участвуют известные представители как науки, так и индустрии, и еще большая аудитория будет действительно внимательно и с интересом читать твою статью. В каждой сфере существует неофициальная градация конференций. Например, в области информационной безопасности и приватности к конференциям первого ранга относятся S&P, CCS, USENIX Security, NDSS, ESORICS, PETS, WWW. Опубликовать статью в сборниках материалов таких конференций – означает пройти строгий отбор и доказать, что твоя исследовательская работа очень важна. Моментально возникает азарт, как в спорте. Я бы очень хотел, чтобы представители наших вузов активнее участвовали в подобных конференциях, тем самым интегрируясь в международную научную работу. А начать можно с кооперации с более опытными коллегами из западных университетов и лабораторий!

• **Во-вторых**, действительно, студентов нужно заинтересовывать практическими исследованиями (настоящим и качественным R&D), которые будут привлекательными для представителей индустрии и других спонсоров. Это не означает, что нужно отказываться от теоретической науки, но любое исследование должно предоставлять и полезный опыт в разработке. В идеале между преподавателями и студентами всегда должен вестись конструктивный диалог об интересах последних и о том, как их работа на кафедре может стыковаться с профессиональным ростом и работой в ИТ-компаниях.

КАК СОЗДАТЬ СТАРТАП?

Уверен, что многие специалисты в области компьютерных наук хотели бы создать свой успешный стартап. А вот насколько в этом способна помочь научная деятельность в университете для студентов может быть не столь очевидно. Многие выбирают работу в крупной ИТ-компании, чтобы сначала набраться опыта и накопить финансовые ресурсы, а потом уже думать об инновационных идеях. К сожалению, по крайней мере моя практика показывает, что прийти к стартап-деятельности по такому пути довольно тяжело. Даже если вы сами являетесь главой аутсорсинговой компании, очень трудно выделить сотрудникам время на внутренние проекты и инновации, ведь все это связано со значительными рисками. Конечно, есть и другие сценарии. Компании могут сотрудничать с аспирантами и докторантами, работая над инновационными технологиями, могут поддерживать исследовательские лаборатории и студенческие конкурсы стартапов. Со стороны университетов при этом нужна поддержка в сфере действительно прикладной науки, в проектах, которые могут вырастать в индустриальные спин-офф компании.

Взгляд PhD студента западного университета замечает и много положительного в украинской науке и ИТ-индустрии. Я действительно горд за нашу математическую подготовку, за наших опытных и мудрых преподавателей и за наших многочисленных талантливых программистов. Это означает, что у нас есть замечательная база, и, ориентируясь на западный формат кооперации и стимулирование инноваций, мы можем достичь очень многого в Украине.

Алексей СТАРОВ

Stony Brook University
Нью-Йорк
PhD candidate
in Computer Science,
PragSec Lab
(Выпустник ХАИ)

ВОВЛЕЧЕНИЕ СОТРУДНИКОВ ИТ-КОМПАНИИ В R&D В СФЕРЕ ИТ-БЕЗОПАСНОСТИ: ПРОБЛЕМЫ И ПОДХОДЫ К РЕШЕНИЮ

Сегодня ни одна из современных ИТ-компаний не может развивать свой бизнес без внедрения инноваций, проведения исследований и разработок (I&R&D - innovation&research&development) в области технологий, которые лежат в основе продукта или сервиса, предоставляемого компанией. Умный бизнес рассматривает инновацию как концепцию развития, роста активов и ресурса, позволяющего выжить в жестких условиях конкурентной борьбы и изменений рынка. Чтобы достигать свои бизнес-цели, необходимы инвестиции в новые продукты и услуги, в усовершенствование самих бизнес-процессов. Это не исключение и для высокотехнологичных компаний, работающих в сфере ИТ-безопасности.

Евгений БРЕЖНЕВ

К.т.н., снс, доцент
Кафедра компьютерных систем и сетей,
Национальный аэрокосмический университет им. М.Е. Жуковского «ХАИ»

Автор 2 книг, 75 научных работ. С 2015 г. менеджер по качеству компании ПАО «НПП «Радикс», г. Кировград. Компания специализируется на разработке приложений, важных для атомной безопасности.

Традиционно ИТ-компании, работающие на рынке Украины, можно разделить на два больших класса – продуктовые компании (компании полного жизненного цикла ИТ-продукта) и компании для ИТ-аутсорсинга. По разным оценкам, в Украине насчитывается порядка 4000 ИТ, 85% из них – это компании малого и среднего бизнеса с численностью персонала менее 80 человек. Эти компании предоставляют интеллектуальный сервис своим заказчикам.

В 2015 году среди украинских ИТ-компаний, работающих на аутсорсинг, просматривается тенденция повышения сложности ИТ-продукта, что говорит о росте профессионализма и квалификации персонала. Как правило, компании обладают высоким интеллектуальным потенциалом, большим количеством собственных наработок, которые могли бы быть использованы как для заказчика, так в интересах самой компании.

Несмотря на жесткие требования рынка, ИТ-компании, работающие на рынке Украины, не стремятся развивать свою I&R&D составляющую. Возникает парадоксальная ситуация. С одной стороны, накапливается потенциал, опыт, идеи, с другой, они так и остаются в голове или на бумаге.

ТЕПЕРЬ Я ХОЧУ ЗАДАТЬ ВОПРОС ВАМ, ЧИТАТЕЛЬ, И ВМЕСТЕ ПОРАЗМЫШЛЯТЬ, ПОЧЕМУ ЭТО ПРОИСХОДИТ ИМЕННО ТАК?

Почему это устраивает ИТ-компании? Ответов много: это удовлетворяет заказчика, незрелость R&D решений, отсутствие ресурсов на их доработку, пр. Что мы имеем в итоге – компания – аутсорсер будет всегда выполнять те незначительные функции, которые передал ей заказчик, дабы избавить своих сотрудников от рутинной работы. Мне кажется, это печальная перспектива. А вам?

ЕСЛИ ВЫ НА ИТ-АУТСОРСЕ И ВАС ТАКЖЕ УСТРАИВАЕТ ТАКОЕ ПОЛОЖЕНИЕ, ТО Я ПРЕДЛАГАЮ ОТЛОЖИТЬ ЧТЕНИЕ И ЗАНЯТЬСЯ БОЛЕЕ ВАЖНЫМИ ДЕЛАМИ.

Если же вы думаете, а что же будет с вашей компаний в будущем и как можно вырваться из роли аутсорсера, то давайте продолжим наши размышления.

Я считаю, что аутсорсинг – это начальная стадия развития ИТ-бизнеса в любой отдельно взятой стране. В идеальном случае, рано или поздно, заказчик может принять решение об изменении вашей роли, о переходе из статуса поставщика интеллектуальных услуг в статус поставщика инновационных услуг. Если это будет так, вашей компании повезло. Будет рост инвестиций, новые предложения, пр.

А если нет? Это более сложный сценарий. Здесь нужно постоянно говорить с заказчиком об этой возможности, о том, что вы хотите и можете давать больше вашему заказчику, или еще больше, вы хотите внедрить культуру инноваций в вашей компании. Это потребует времени, но вы же хотите роста инвестиций в вашу компанию?.....

Можно предположить, что все же, если заказчик примет решение и даст вам возможность сделать первые шаги в направлении инноваций, то первое, с чего следует начать ее R&D менеджеру – это провести анализ опыта организации подобного процесса в Украине, с учетом наших реалий, проблем и лучших практик.

КАКИМ ОБРАЗОМ ИТ-КОМПАНИЯ МОЖЕТ ВНЕДРИТЬ ИННОВАЦИОННУЮ КУЛЬТУРУ СРЕДИ СВОИХ СОТРУДНИКОВ?

Основными и общепринятыми методами являются: разработка и внедрение инновационной стратегии, повышение компетенций персонала, раскрытие креативного потенциала, обмен идеями, инвестиции в инновации, пр. Это всегда должно идти от топ-менеджмента компании или, как минимум, находить у них поддержку. Это движение сверху вниз.

А можно ли двигаться снизу вверх?

Опыт внедрения инноваций на примере украинских продуктовых ИТ-компаний показывает, что можно. Дополнительным методом внедрения инноваций (снизу вверх) является вовлечение молодых сотрудников в исследования и разработку, а проще сказать, в науку.

Как сделать так, чтобы молодые ИТ-специалисты не боялись науки, стремились к инновациям, находили бы время для исследований в области используемых технологий?

Вопрос сложный и неоднозначный и не единожды заданный этим же специалистам. Реакция на вопрос различна: от улыбок до недоумения...

В качестве положительного примера движения снизу вверх в направлении внедрения инновационной культуры можно рассмотреть опыт сотрудничества ПАО «НПП «Радий» (далее Радий) и Национального аэрокосмического университета «ХАИ» (кафедры компьютерных систем и сетей, далее КСС). Это длительный путь, с преодолением барьеров, ошибками, с поиском лучших, наиболее приемлемых форм кооперации.

Итак, с чего начать компании, которая хочет пойти в инновации снизу вверх, путем кооперации с университетом? Уже сегодня понятно, как можно было бы избежать множества ошибок.

Залогом успешной кооперации является создание благоприятной системы сотрудничества, так называемой экосистемы (☺модное слово). Эта экосистема (см. рис 1.), должна включать:

- общую стратегию вовлечения сотрудников компании в науку;
- общие подходы и формы их вовлечения;
- перечень совместных активностей для вовлечения ИТ сотрудников в науку.

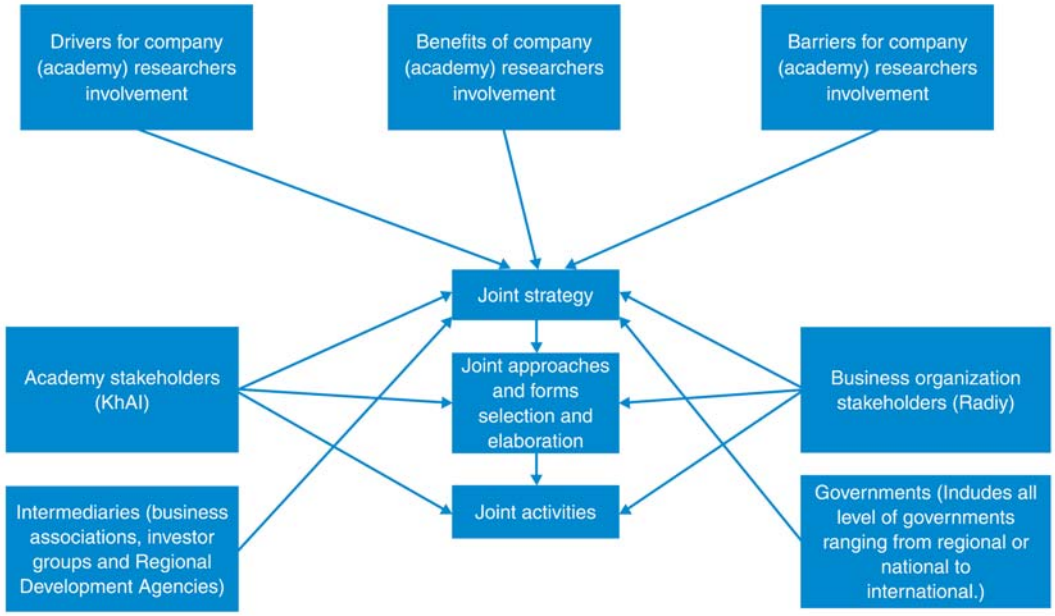
Экосистема должна включать всех стейкхолдеров (университет, компании (отделы), местные органы власти, организации и фонды, пр.). Радий и КСС определили перечень мотиваторов, возможных проблем и выработали подходы к их решению.

К ОСНОВНЫМ МОТИВАТОРАМ ДЛЯ КОМПАНИИ МОЖНО ОТНЕСТИ:

- профессиональное развитие персонала, рост знаний и компетенций;
- экономия средств за счет только внутренних инвестиций (не нанимаются внешние компании для проведения исследований);
- создание благоприятной среды для развития и внедрения инновационной корпоративной культуры компании;
- развитие технологий, продуктов и сервисов, пр.
- поиск перспективных кадров среди молодежи в университетах.

РИСУНОК 1

ЭКОСИСТЕМА ДЛЯ ВОВЛЕЧЕНИЯ ИТ ПЕРСОНАЛА КОМПАНИИ В НАУКУ



К ОСНОВНЫМ МОТИВАТОРАМ ДЛЯ УНИВЕРСИТЕТА МОЖНО ОТНЕСТИ:

- благоприятное влияние на учебный процесс, который становится ориентированным на современные проблемы и технологии в индустрии;
- создание банка тем и работ для проведения бакалаврских (магистерских работ);
- использование представителей ИТ-компаний как преподавателей;
- обмен знаниями путем проведения тренингов, семинаров, пр.

Первоначальными совместными шагами на пути создания этой экосистемы были:

1. Выработка общего видения. Зачем нам это нужно?

Общим видением для Радия и КСС является – создание общей экосистемы для развития персональных навыков и умений, постоянного обучения с целью удовлетворения требований бизнеса и общества.

2. Далее, сложное и, увы, не всегда возможное. Нужны люди, увлеченные фанатики, которые хотят продвигать кооперацию.

3. Если задача 2 решена, то далее просто необходимо определить препятствия, цели, пользу, пр., а также не забыть все заинтересованные стороны. Не забыть о двух главных целях: первая – «поставить на землю» молодых ученых из университетов, сделав их темы максимально практическими, вторая – мотивировать представителей ИТ-компании помочь увидеть науку рядом с ними, в области их деятельности.

4. Далее определить формы, подходы, методы (как все делать?).

5. Определить каналы коммуникации.

6. И, главное, определить план действий. Набор понятных совместных активностей (семинары, конференции, выступления, пр.).

Радий и КСС сотрудничают в науке уже более 10 лет. Очень приятно отметить, что это дерево кооперации на сегодняшний день дало уже много плодов, а именно:

КОНФЕРЕНЦИИ

Радий является спонсором – компанией, которая поддерживает проведение ежегодной международной конференции DESSERT Conference – DEpendable System, SERvices and Technologies, посвященной актуальным проблемам применения ИТ-технологий в области критических приложений. Многие молодые ученые компании имеют возможность выступить на конференции, обсудить важные проблемы науки и практики.

В свою очередь молодые ученые КСС принимают активное участие в международном семинаре по применению ПЛИС (программируемых логических интегральных схем) для ИУС (информационно-управляющей системы) критических приложений.

ЛАБОРАТОРИИ

Кооперация Радия и КСС позволила создать ряд небольших научных лабораторий, в которых сотрудники Радия имеют воз-

можность помогать студентам и молодым ученым КСС. Так, например, в 2013 году была создана лаборатория мобильных и беспроводных технологий. Студенческая лаборатория мобильных и беспроводных технологий основана на базе кафедры компьютерных систем и сетей в 2013 в рамках проекта «Green Computing & Communications» (Project Number: 530270-TEMPUS-1-2012-1-UK-TEMPUS-JPCR).

ОСНОВНЫМИ ЗАДАЧАМИ ЛАБОРАТОРИИ ЯВЛЯЮТСЯ:

- Поддержка учебного процесса по направлениям беспроводных и мобильных технологий. Оборудование лаборатории используется при выполнении лабораторных и практических работ, связанных с разработкой приложений с использованием беспроводных и мобильных технологий.
- Проектная деятельность. Разработка мобильных и беспроводных приложений совместно с представителями ИТ-компаний.
- Проведение научных исследований по направлениям: анализ сенсорных сетей, оптимизация параметров систем управления освещением, анализ беспроводных технологий передачи данных, оценка и обеспечение информационной безопасности, пр.
- Организация и проведение тренингов по направлениям деятельности лаборатории.

НАПИСАНИЕ КАНДИДАТСКИХ ДИССЕРТАЦИЙ

В настоящее время на Радии насчитывается более 10 кандидатов наук. Восемь из них защитились на КСС. Темы работ соответствовали области общих научных интересов КСС и Радия. Среди них: методы многоверсионного резервирования и инструментальные средства проектирования отказоустойчивых систем на ПЛИС, методы и модели для оценки гарантоспособности ИУС АЭС, пр.

К результатам, подтверждающим эффективное внедрение инноваций (снизу вверх), по вовлечению молодых ученых ИТ-компании в науку можно добавить: регулярные совместные публикации в национальных и международных рейтинговых журналах, доклады на конференциях, пр. Можно также похвастаться (в хорошем смысле, без ложной скромности) организацией и проведением совместных семинаров, хакатонов по безопасности, организацией стартапных конкурсов.

Еще один важный вопрос – как можно оценить в денежном эквиваленте такой способ движения в направлении инноваций ИТ-компании в кооперации с вузом?

Компания не нанимает R&D аутсорсера, компания развивает свой персонал, повышая компетенции персонала, компания получает готовые решения, которые помогают решать реальные задачи бизнеса. Т.е. умный бизнес создает свой R&D центр, инвестируя в свое будущее.

Таким образом, если ваша ИТ-компания решила стать на рельсы внедрения инноваций, то это здорово! Это залог успеха вашего бизнеса, инвестиции в будущее вашей компании. Путей может быть много, но успех один. Он приходит только к тем, кто идет вперед, вовлекая персонал компании в инновации. Описанный опыт может быть уникальным и неповторимым. Он содержит основные вехи, описывает путь отдельной компании и университета.

Просто поверьте, что вовлечение ИТ-персонала в науку нужный и необходимый шаг. Идите в университеты! Сделайте этот шаг! ■

ОТ СУПЕРКОМПЬЮТЕРА – К ПОСТРОЕНИЮ ЦЕЛОСТНОЙ КАРТИНЫ МИРА

Интервью с украинским ученым Александром Васильевичем Палагиным, академиком НАН Украины, заместителем директора Института кибернетики им. В.М. Глушкова НАН Украины.

Александр Васильевич ПАЛАГИН

Академик НАН Украины,
заместитель директора Института кибернетики им. В.М. Глушкова НАН Украины

Карт Бланш: Уважаемый Александр Васильевич! Спасибо, что Вы нашли время для нашего интервью. Расскажите, пожалуйста, о достижениях и приведите примеры успешных практик в создании и внедрении технологий, разработанных Вашим институтом. Какими Вам видятся перспективы в рассматриваемой области?

Александр Васильевич: Можно назвать несколько сильных результатов, которыми гордится Институт. Первый из них относится к суперкомпьютеру, его развитию и созданию на его основе информационных технологий трансвычислительной сложности. Суперкомпьютерный комплекс СКИТ4, хотя и небольшой производительности по современным меркам (43 Тфлопс – пиковых, 160 ТБайт), но обслуживает все институты Академии НАН Украины и ряд государственных организаций, а также является ресурсным центром украинского Грида. На нем решают до 50 тыс. задач в год специалисты в области физики, математики, молекулярной биологии, экономики и др. Ученые Института являются мировыми чемпионами в решении задач оптимизации трансвычислительной сложности.

Очень интересные результаты получены в создании магнитокардиографических систем высокой диагностической точности. Они уже нашли свое место в клиниках Украины, Германии, Китая. Успешными в применении оказались также электрокардиографические комплексы с новыми функциональными возможностями.

Можно отметить также область компьютерного приборостроения. Созданный нашими учеными прибор «Флоротест», позволяющий выполнять экспресс-диагностику состояния растений, заинтересовал специалистов агротехнического и экологического профилей. Выпускаемые Инженерным центром Института малыми партиями приборы хорошо зарекомендовали себя в среде профессионалов, как в Украине, так и за ее пределами. Проект УНТЦ (Science and Technology Centre in Ukraine, http://www.stcu.kiev.ua/) по тиражированию этих приборов оказался весьма кстати в сегодняшней сложной ситуации Академии.

Хорошо известны результаты применения системы «Надра» при анализе сос-

тояния подземных вод и земной коры в интересах строительной отрасли и экологических приложений.

На этом не заканчивается список серьезных научных разработок Института. Идея академика Б.Е. Патона относительно «целенаправленных» научных исследований по-прежнему актуальна и востребована.

Остаются проблемы внедрения результатов научных исследований и создания структурных подразделений и организаций, непосредственно работающих с промышленностью и бизнесом, предпроектного маркетинга, виртуальных научных инновационных центров с сильной государственной поддержкой.

Карт Бланш: Вы – известный ученый в области кибернетики и информационных технологий – в последнее время активно занимаетесь проблемой трансдисциплинарных исследований. С чем это связано? Как такие исследования могут повлиять на развитие ИТ?

Александр Васильевич: Современный этап развития науки и ее приложений носит явно трансдисциплинарный характер. Этот факт обусловил необходимость разработки строгой методологии трансдисциплинарных (ТД) научных исследований, создания ТД-международных центров и школ, наконец, определения места и роли информатики в системно-технологической поддержке ТД-исследований и использования их результатов при решении глобальных проблем развития современной цивилизации. ТД-парадигма предполагает построение в обозримом будущем общей научной картины мира или, что то же самое, – единой ТД-системы знаний, обеспечивающей формализованные постановку и решение конкретных задач при выполнении комплексных проектов высокой сложности, социальной значимости и конкурентности.

Серьезным фактором, определяющим место и роль науки в жизни общества, является то, что она пока не располагает целостной картиной мира. В связи с этим ей свойственны частичные проекции сущего бытия под углом зрения частных научных дисциплин, постигающих те или иные законы природы в зависимости от проблемной ориентации исследований.

Вместе с тем эпоха аналитизма и свойственная ей дифференциация науки и замкнутых научных теорий уже позади. Стало очевидным, что реальные проблемы, стоящие перед человеческим обществом, гораздо сложнее научных, и наука не в состоянии их кардинально решить вследствие разобщенности научных дисциплин и их специализации, слабой координации научных коллективов и их тематики, отсутствия общего формализованного языка представления знаний.

Трансдисциплинарные исследования, захватывая зоны пограничных (демаркационных) ареалов научных дисциплин, интегрируют сущностные основы последних, образуя так называемые кластеры конвергенции, в которых происходит мощное синергетическое взаимодействие за счет взаимопроникновения парадигм и конкретных текущих результатов каждой из дисциплин, входящих в тот или иной кластер. Указанное взаимодействие отражает целостность реального мира, являясь стимулом и одновременно гарантией успешности ТД-исследований и связанных с ними практических проектов, нетривиальности и значимости их результатов.

Таким образом, *сущность трансдисциплинарного подхода* заключается в эффективном обеспечении двуединства концепций углубления конкретных знаний в предметной области, с одной стороны, и расширения охвата проблемы, исходя из реальности единства мира и стремления воссоздать его целостную научную картину, – с другой. Он реализуется через интеграцию исходных научных теорий путем обмена понятиями и методами разных наук, формировании новых понятий и теорий. Они расширяют диапазон трансдисциплинарности в направлении построения глобальной интегрированной системы знаний, которая не просто фиксирует научную картину мира, но и является активной средой, обеспечивающей решение конкретных научно-технических задач и развитие самой системы знаний.

Компьютерные онтологии являются интенсивно развивающимся в настоящее время разделом информатики как теоретической, так и практической (возник даже раздел инженерии знаний, названный онтологическим инжинирингом). Актуальность данного направления представляется очевидной в связи с двумя главными обстоятельствами.

Первое из них связано с тем, что компьютерные онтологии являются одновременно и результатом развития, и инстру-

ментом knowledge-engineering, т.е. они выступают в качестве средства концептуализации научной теории, а также спецификации и формализации баз знаний предметных областей, выполняя функции классификации, структурирования, упорядочения, интеграции и инструмента при использовании знаний.

Второе обстоятельство связано с функциями онтологий в пространстве современных знаний. Речь идет о построении эффективного механизма поиска релевантной запросу пользователя информации, исходя из его первичной системы знаний в предметной области и адекватного отображения объекта его интересов в структурированные семантические модели, связывающие базовые концепты отношениями порядка (род – вид, класс – подкласс, часть – целое, объект – свойство и др.), и более сложные устойчивые конструкции для организации запросов в Интернете.

Общая задача онтологии – скомпенсировать отсутствие стандартов на представление знаний при взаимодействии пользователя с информационными системами и последних между собой. В качестве основных онтолого-управляемых функций можно назвать:

- эффективное компактное представление и отображение системы знаний конкретной предметной области на базе современных ИТ;
- поиск необходимой информации в пространстве Интернета;
- интегрирование знаний в одной или нескольких предметных областях;
- развитие системы и получение новых знаний (либо упорядочение существующих, проверка их непротиворечивости, коррекция) и др.

Все указанные функции реализуются в специальном классе знание-ориентированных интеллектуальных компьютерных систем (ИКС), а именно, онтолого-управляемых ИКС.

Теория и практика создания и использования систем, основанных на знаниях, – актуальное и интенсивно развивающееся направление Computer Science, позволяющее повысить эффективность компьютерных технологий, прикладных систем, инструментальных средств. Сложность проблемы определяется, в частности, сложностью построения, организации и использования больших баз формализованных знаний, а также привлечением целого ряда научных теорий (логики, компьютерной лингвистики, нейрокибернетики, теории семантических сетей и др.), которые составляют основу *теории трансдисциплинарных научных исследований*.

Карт Бланш: Совершенствование и внедрение новых технологий сейчас невозможно без кооперации с ИТ-индустрией и индустрией вообще. Известны модели такой кооперации университетов и индустрии, разрабатываемые и внедряемые в рамках европейского проекта TEMPUS-CABRIOLET, в выполнении которого принимает участие Институт кибернетики. В чем специфика кооперации Национальной Академии наук с ИТ-индустрией в деле создания и коммерциализации новых технологий?

Александр Васильевич: С принятием нового закона о науке, по сути, начался поиск форм и методов взаимодействия науки, образования, индустрии и рынка. Речь идет не только о простом выживании в условиях глубокого экономического кризиса, но и переходе на инновационный путь развития, где наука и образование являются главными стимулирующими факторами развития. В этих условиях сближение науки и образования, совместный поиск прорывных направлений развития, в том числе, в ИТ, является определяющей стратегией движения вперед.

Опыт, полученный при выполнении проекта TEMPUS-CABRIOLET, – лучшее подтверждение сказанного. На самом деле, подготовка специалистов, опыт их участия в исследованиях и разработке технологий, создание комплексных команд с участием зарубежных профессионалов высокого уровня, не могут быть переоценены. Примером может служить только что состоявшаяся школа на базе Королевского технологического университета (Стокгольм), где, в частности, обсуждались проблемы и результаты создания Smart City, которая нашла свое отражение в Европейской программе «Горизонт 2020» и весьма актуальна для Украины. Проектная команда от Украины, в которую входят несколько технических университетов Харькова, Николаева, Одессы, Чернигова, Черновцов, а также университетов Великобритании, Италии, Португалии, Швеции, вместе с ИТ-компаниями и академическими институтами отрабатывает и внедряет реальные модели кооперации.

R&D для ИТ-БЕЗОПАСНОСТИ

- Безопасность атомной ИТ-индустрии: путь через R&D
- R&D в кибербезопасности: опыт Эллады
- Криптозащита: все сначала?

АЭС:
25 ЛЕТ ИССЛЕДОВАНИЙ И ПРАКТИЧЕСКИХ РЕЗУЛЬТАТОВ

University-Industry Cooperation в Украине в области обеспечения и оценивания безопасности информационно-управляющих систем.

Атомная энергетика – сегмент особо пристального внимания в экономической и социально-политической жизни любого государства. Атом может быть мирным, созидающим, но его энергия может стать и разрушительной, нанести непоправимый вред окружающей среде – нашему общему природному дому, а также жизни и здоровью людей – самому важному ресурсу любой страны. И здесь на помощь мирному атому должны прийти ученые, исследователи, глубоко осознающие степень возложенной на них миссии гармонизации безопасного сосуществования человека и атома на нашей общей зеленой планете.

Украина – особая страна, со своей особой миссией. Относительно небольшая страна подарила миру большое количество открытий в области атомной энергетики. И этой же стране суждено было испытать последствия самой страшной в истории человечества Чернобыльской катастрофы, произошедшей 30 лет назад. Поэтому, с осознанием своей особой миссии, Украина занимает важное место в исследованиях, относящихся к безопасности атомных электростанций (АЭС).

АЭС в Украине производят около 50% электроэнергии, что определяет ее стратегическое положение среди других отраслей. Функционируют 15 реакторов на Запорожской, Ровенской, Южно-Украинской и Хмельницкой АЭС с суммарной мощностью в 13 880 МВт. Украина входит в топ-5 крупнейших производителей атомной энергии в Европе и TOP10 в мире. Естественным требованием к АЭС является ограничение негативного влияния на окружающую среду и персонал.

Развитие информационных технологий привело к их широкому внедрению на АЭС. Важной задачей является обеспечение безопасной эксплуатации цифровых информационно-управляющих систем (ИУС), являющихся, в свою очередь, ключевым звеном безопасности станций.

Обеспечение и оценивание безопасности АЭС осуществляется в треугольнике «эксплуатирующая организация (несет основную ответственность за безопасную эксплуатацию) – поставщик (несет ответственность за разработку и производство безопасного оборудования) – регулирующий орган (является государственной организацией, отвечающей за государственное регулирование, независимую оценку и выдачу разрешительных документов по эксплуатации)». Регулирующим органом является Государственная инспекция ядерного регулирования Украины, а непосредственную работу с АЭС и поставщиками проводят организации технической поддержки. Одна из них – Государственный научно-технический центр по ядерной и радиационной безопасности (ГНТЦ ЯРБ).

После получения Украиной независимости следовало создать собственную структуру, способную на должном уровне осуществлять техническую поддержку государственного регулирования в области безопасности ИУС АЭС. Для этого был создан Харьковский филиал (ХФ) ГНТЦ ЯРБ, который более 20 лет возглавлял заслуженный деятель науки и техники Украины, доктор технических наук профессор М.А. Ястребенецкий. Деятельность Центра включала: совершенствование нормативной базы и приведение ее в соответствие с международными стандартами; оценивание и повышение безопасности всех ИУС АЭС путем выполнения государственных экспертиз (проведено сотни экспертиз); участие в международных проектах, связанных с обеспечением и оцениванием ЯРБ. Эти задачи решались и решаются с участием сотрудников университетов. Особенностью ХФ ГНТЦ ЯРБ было постоянное развитие University-Industry Cooperation (UIC) - участие в совместных конференциях, семинарах; преподавание в вузах; привлечение к сотрудничеству специалистов вузов в области безопасности и надежности, в частности, в 1995 г. и 2001 г. были приглашены в качестве экспертов авторы этой статьи.

В 2003 г. в журнале «Ядерная и радиационная безопасность» была опубликована статья Харченко В.С., Ястребенецкий М.А., Скляр В.В. «Новые информационные технологии и безопасность информационно-управляющих систем АЭС», определившая дальнейшие направления в области нормативного регулирования ИУС АЭС с учетом внедрения новой элементной базы, включая программируемые логические интегральные схемы (ПЛИС), расширения роли и номенклатуры используемого программного обеспечения, развития международной нормативной базы, новых технологий и принципов разработки ИУС АЭС.

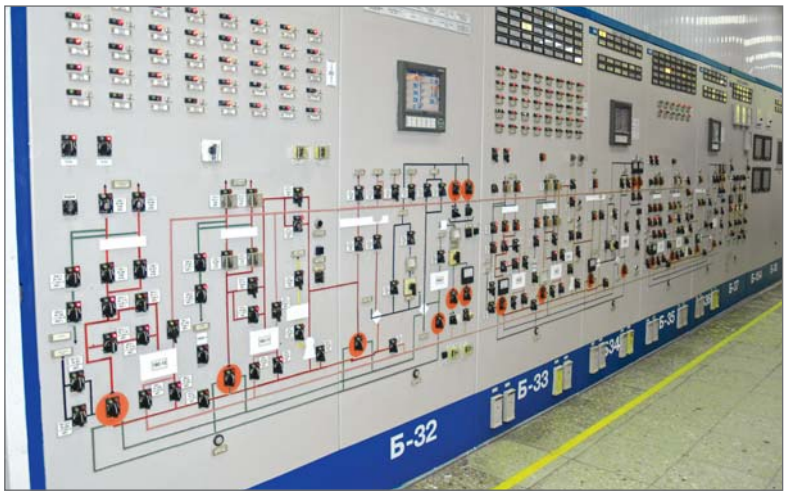
Следует отметить, что ко многим из исследований, выполненных в рамках обозначенных направлений, применимо определение «впервые в мире» или «одни из первых в мире». Так, впервые было выполнено обоснование структуры и процессов жизненного цикла безопасности ИУС АЭС на базе ПЛИС. Результаты исследований были использованы при проектировании и оценивании безопасности нового поколения ИУС АЭС на базе ПЛИС, разработанных НПП «Радий», таких как системы аварийной и предупредительной защиты реактора, автоматического регулирования, разг-

Вячеслав ХАРЧЕНКО

Заслуженный изобретатель Украины, д.т.н., профессор, заведующий кафедры компьютерных систем и сетей ХАИ, директор НТЦ исследования и анализа безопасности инфраструктур НПП «Радий»

Владимир СКЛЯР

Д.т.н., профессор кафедры компьютерных систем и сетей ХАИ



Панели из состава управляющей системы безопасности, Ривненская АЭС, энерноблок 2, система произведена НПП «Радий».

рузки и ограничения мощности реактора, группового и индивидуального управления регулирующими органами реактора, нормальной эксплуатации реакторного и турбинного отделений и др. Результаты украинских разработок были в дальнейшем внедрены в положения стандартов Международной электротехнической комиссии (например, IEC 62566:2011 Nuclear power plants – Instruments and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions) и учтены в практиках национальных регулирующих органов. Например, регулирующий орган США выпустил в 2009 г. технический отчет EPRI TR-1019181 Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems, учитывающий украинский опыт оценивания и обеспечения безопасности ИУС АЭС на базе ПЛИС.

Еще одним важным направлением являлось обоснование диверсности ИУС АЭС, разработанной на базе ПЛИС. Впервые было проведено оценивание и обоснование безопасности системы управления и защиты реактора, в которой диверсные комплекты АЗ-ПЗ были выполнены с применением разных программно-аппаратных средств с использованием различных типов ПЛИС. Подобный подход был внедрен на всех 15 энергоблоках АЭС Украины и подтвержден более чем десятилетней безопасной эксплуатацией.

Проведенные исследования во многом определи успешное лицензирование, внедрение и эксплуатацию ИУС на энергоблоках украинских АЭС. В 2004 г. в Украине были введены в эксплуатацию два новых энергоблока – Ровно-4 и Хмельницкий-2, на которых были применены ИУС нового поколения, в том числе и на базе ПЛИС.

Полученные за годы деятельности практические и теоретические результаты обобщены в монографиях «Безопасность атомных станций: информационны и управляющие системы» (2004) и «Системы управления и защиты ядерных реакторов» (2011), выпущенных киевским издательством «Техніка» под редакцией Ястребенецкого М.А. и Харченко В.С. В 2014 г. в США под их редакцией вышла монография NPP Instrumentation and Control Systems for Safety and Security, подготовленная совместно сотрудниками ГНТЦ ЯРБ, НПП «Радий» и ХАИ.

Важным событием в области UIC было создание в 2007 г. на базе кафедры компьютерных систем и сетей ХАИ научно-технического центра исследования и анализа безопасности инфраструктур (НТЦ ИАБИ), в основу деятельности которого положена модель spin off компании (разновидность дочерней компании). Центр был создан для поддержки деятельности НПП «Радий» при лицензировании и сертификации ИУС АЭС в Украине и за рубежом. Чем уникальна эта организация среди немногочисленных «коллег по цеху»? Прежде всего, принципами реализации возложенной на сотрудников миссии. Принципы эти – изучение и применение базы самых высоких международных стандартов в своей сфере, преемственность научных школ разных поколений, максимально тесная связь теории базы и четкого осознания практических целей и методов их применения. Молодые ученые, осознающие значение исследований, и при поддержке своих наставников гораздо эффективнее могут внед-

рять результаты исследований в быстро меняющемся современном мире. Соединение воедино научного и бизнес-ориентированного опыта в области технического консалтинга позволило получить уникальные для украинского и мирового рынка результаты.

Первым крупным проектом, выполненным с участием НТЦ ИАБИ, являлась поддержка лицензирования УСБ (управляющей системы безопасности), разработанной и поставленной НПП «Радий» для АЭС Козлодуй (Болгария, 2008-2010 гг.). Это был крупнейший контракт, выполненный украинским предприятием на сумму более 100 млн евро.

В основе достижений НТЦ ИАБИ отметим следующие подходы к UIC: построение долговременных отношений с владельцами бизнеса и его общее понимание; выполнение нескольких небольших успешных проектов, предшествующих крупному проекту; значительный опыт и экспертные знания по предполагаемым направлениям деятельности (в данном случае – в надежности и безопасности ИТ); наработка навыков, которые могут быть потенциально востребованы индустрией; наращивание опыта международной деятельности и знание английского языка. Будучи практиками в области UIC, сотрудники НТЦ ИАБИ, кроме решения задач лицензирования и сертификации, развивали следующие направления: разработка концепции и запуск Украинского UIC агентства; постоянный диалог между представителями индустрии и университетов, выполнение совместных проектов продвижения в Украине концепции UIC, в частности, регулярное проведение в Украине семинаров BASiC (Workshop on Business Analysis and Project Management for Innovative Startups in Critical Domains) и других тематических мероприятий; участие в проектах Евросоюза по программе TEMPUS; постоянное участие с 2013 г. в качестве спикеров в международных конференциях University-Industry Interaction Conference (организатор University Industry Innovation Network), других форумах, посвященных UIC; развитие и внедрение практических и теоретических положений концепции UIC.

В 2012 г. с участием сотрудников Полтавского национального технического университета имени Юрия Кондратюка была создана spin off компания Poltava-V&V – дополнительная площадка НТЦ для независимой верификации и валидации НПП «Радий». Здесь разработана и внедрена технология верификации и валидации полного жизненного цикла платформы и ИУС на базе ПЛИС, включая: технические обзоры документации; трассировку требований; статический анализ кода; тестирование, временное и логическое моделирование программных модулей и интегрированного кода; тестирование интегрированных программно-аппаратных средств; тестирование диагностических функций с внесением программно-аппаратных дефектов.

Вячеслав Харченко, Владимир Скляр (Идеи приходят на Капри)

В период 2011-2014 гг. на НПП «Радий» был выполнен первый в мире проект по разработке и сертификации программируемого логического контроллера (ПЛК) на базе ПЛИС.

Последняя технология заслуживает особого внимания, поскольку обладает мировой новизной с точки зрения реализации засева дефектов в платформу безопасности на базе ПЛИС, включая аппаратную часть и программный код.

Таким образом, развитие UIC в области лицензирования и сертификации ИУС АЭС привело к созданию научного направления и школы по обеспечению и оцениванию функциональной безопасности ИТ.

Следует отметить ряд инновационных проектов, выполненных на НПП «Радий» в рамках UIC при поддержке НТЦ ИАБИ и Poltava-V&V (представлены ниже).

Блочный щит управления энергоблока 2 Ривненской АЭС после модернизации, выполненной с участием НПП «Радий» в 2008 г.

В период 2011-2014 гг. на НПП «Радий» был выполнен первый в мире проект по разработке и сертификации программируемого логического контроллера (ПЛК) на базе ПЛИС. Данная платформа получила название RadICS. Сертификация осуществлялась на соответствие требованиям стандарта МЭК 61508, который реализует наиболее высокий уровень требований по безопасности к программируемым компонентам и системам.

В 2013-2014 гг. НПП «Радий» заключил контракты с канадской компанией Candu Energy (разработчик тяжеловодного реактора CANDU) на проектирование и производство двух систем безопасности на базе ПЛИС для аргентинской АЭС Эмбалсе: аварийной сигнализации щитов управления и измерения скорости вращения главного циркуляционного насоса. В этом проекте НПП «Радий» впервые реализовал лицензирование ИУС АЭС на базе ПЛИС по требованиям Канады и Аргентины.

В 2014-2015 гг. НПП «Радий» выполнил исследовательский проект в партнерстве с Electricite de France по разработке и изготовлению тестового прототипа для изучения контроллера на базе ПЛИС. Несмотря на исследовательский характер проекта, для разрабатываемой ИУС был реализован жизненный цикл согласно стандартам, применяемым в лицензионной практике во Франции.

В 2015-2016 гг. НПП «Радий» разработал систему управления исследовательским реактором для научно-исследовательского института CNEN-IPEN (Бразилия). Лицензирование системы выполнялось согласно регулирующим требованиям Бразилии.

С 2015 г. НПП «Радий» проводит работы по сертификации платформы RadICS согласно требованиям регулирующего органа США (Nuclear Regulatory Commission, NRC). Данная программа рассчитана на несколько лет, поскольку в рамках данной сертификации предъявляются достаточно жесткие требования к продукту, в особенности, к процессу жизненного цикла и к тестированию на устойчивость к внешним воздействующим факторам.

Несмотря на достигнутые успехи, дальнейшее развитие UIC в рассматриваемой области сопряжено с рядом проблем, прежде всего, кадровых. Усложнение ИУС АЭС приводит к тому, что для их оценивания необходимы все более глубокие инженерные знания. В то же время специалисты предпочитают трудоустройство в области ИТ, характеризуемой более высокими зарплатами и не таким уровнем ответственности. Непосредственная подготовка специалистов в области безопасности ИУС и ИТ (safety engineer) в Украине не выполнялась. В ХАИ подготовка бакалавров и магистров по cyber security / safety начата с 2012 г.

Тем не менее, накопленный опыт UIC в области обеспечения и оценивания безопасности ИУС АЭС позволяет говорить о перспективности дальнейшего сотрудничества в следующих направлениях: кибербезопасность ИУС АЭС, включая композицию свойств security и safety; применение и развитие методологии Assurance Case, включая разработанное в Украине направление Assurance Case Driven Design; разработка моделей эффективного и оптимального распределения ресурсов на сертификацию и лицензирование; внедрение опыта, полученного в международных проектах, в практику лицензирования и сертификации украинского регулирующего органа; дальнейшее развитие теории и практики UIC.

Мир меняется, теории могут устаревать и не успевать за стремительно изменяющимися реалиями. Однако любовь к своему делу и понимание важности практических результатов по-прежнему стоят на страже безопасности и прогресса. ■

INFORMATION SECURITY RESEARCH FOR INNOVATIVE PRODUCT AND SERVICE DEVELOPMENT

The widespread use of information technology in virtually all fields of everyday economic, social, technical, cultural and other human activity, creates ever increasing concerns about the security, reliability and the privacy of any action.

Nikolaos BARDIS and Nikolaos DOUKAS

Informatics LAB
Department
of Mathematics
and Engineering Sciences
Faculty of military sciences
Hellenic Military Academy

Technology users (including industries and nations) are increasingly concerned that technology vendors and powerful governments and organizations possess alternative means of overcoming standard algorithms. Additionally, the Internet of Things paradigm, accentuates the necessity for the development of computationally simple but robust solutions for specialized problems.

The Informatics Laboratory (i-Lab) of the Hellenic Military Academy has presented innovations that provide answers to the above problems and is constantly conducting research towards the direction of proposing tailored algorithms for innovative applications.

The Hellenic Military Academy was founded in 1828 and it is the oldest higher education institution of the Greek state that educated the first engineers in modern Greece. The Informatics Laboratory (i-Lab) is conducting teaching activities that cover the undergraduate and postgraduate courses and the provision of specialized training to external bodies. The main part of the scientific effort pursued by the laboratory is research and development in the fields of Information Security, Cryptography, Cyber warfare and Cyber Security, System Engineering, Operational Research, Signal Processing, Simulation, Software Engineering, Microprocessors and Serious Computer Games. The lab is highly involved in R&D efforts for the benefit of the industrial, financial and government sectors and is actively seeking participation in international research activities. It has especially close ties with Greek higher education institutes such as the University of Athens, the University of the Peloponese, the National Technical University of Athens, the Polythechnic Institute of Crete, the National Center for Research «Democritus» et. al.

TECHNOLOGICAL RESEARCH AND INNOVATION

Members of the Informatics Laboratory have in recent years presented innovative solutions, in answer to problems that arise in specific applications.

- 1. Vulnerability Assessment, Penetration testing or «Ethical Hacking» and Adversaries simulation service

With an ethical hacking service the ability of applications, systems or networks to

NIKOLAOS G. BARDIS

Nikolaos G. Bardis received the diploma of Computer Engineering and the PhD degree from National Technical University of Ukraine (Polytechnic Institute of Kiev) in 1995 and 1999 respectively. He is currently an Associate Professor at the Hellenic Military Academy – Department of Mathematics and Engineering Sciences and the Director of the Informatics LAB at the same institution. Collaborates as a lecturer and researcher at the University of Athens – Department of Mathematics and entered the postgraduate course of Cryptography and Security of Information Systems. His research interests include cryptography and data security, information theory, coding theory, systems engineering and applications in defence. He has published in over 40 peer-reviewed journals and conferences. He is a member of the Technical Chamber of Greece, Technical Program Committee (TPC) of the IEEE Communication Society (COMSOC), IEEE Computer Society Technical Committee on Computer Communications (TCCC), Technical Council on Software Engineering (TCSE) of the IEEE Computer Society and IEEE Information Theory Society.

NIKOLAOS DOUKAS

Nikolaos Doukas, received his BEng (1st class honors), MSc and PhD Degrees from Imperial College, London in 1992, 1993 and 1998 respectively. He is currently an Assistant Professor of Information Technology in the Hellenic Army Academy. He has got extensive teaching experience at the Athens University for Economics and Business, Imperial College, the Hellenic Air Force Academy and the Hellenic Army Academy. His research interests include Cryptography, Data Security, Software Engineering, Decision Support Systems, Data Mining, Blind Source Separation, Ultrasonic Signal and Image Processing, Optimization and e-Learning systems. He has participated in research and development projects supported by the European commission, the UK Ministry of Defence, LG Semiconductors, the Cypriot Government, the Greek Government, Thales Airborne Systems (Thomson CSF – Detexis) and other organisations, while he has also been contributing for over 15 years in the development of commercially available CAD software for architectural design and static analysis of buildings. He has published in over 20 peer-reviewed journals and conferences while he is also co-inventor in a European Patent in 2011, in the field of secure speech communications.

withstand cyberattacks may be evaluated. This involves authorizing an ethical hacker to use current cybercrime techniques against an organizations infrastructure, in order to expose unknown vulnerabilities and their potential effects.

This differs from vulnerability scanning that is a largely automated process for evaluating documented vulnerabilities misconfigurations or weaknesses. Penetration testing, is a manual process that may use automated and custom tools, but the foundation of the work is human ingenuity and skills. I-lab is experienced in ethical hacking and adversaries simulation services.

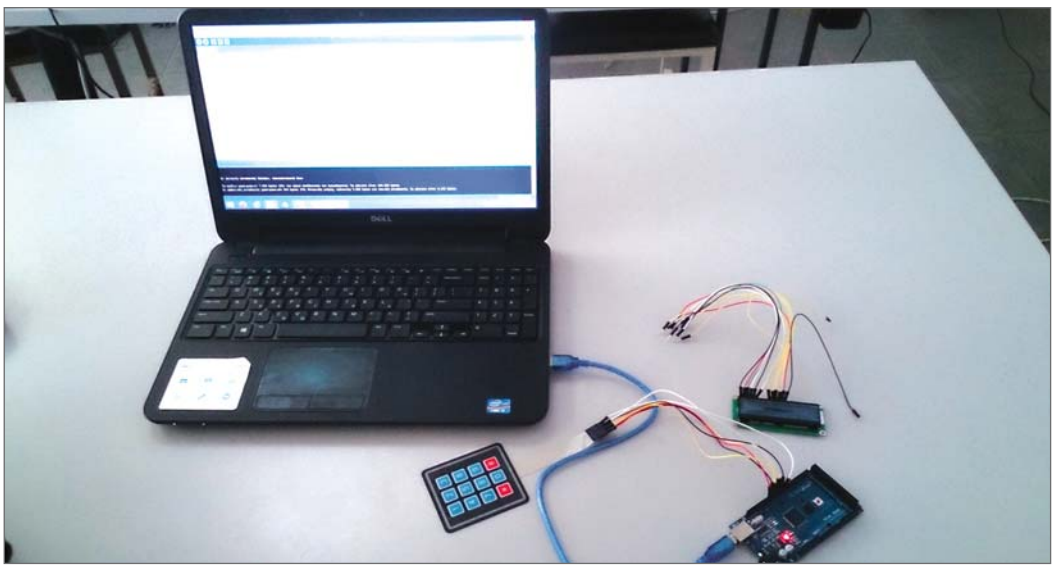
- 2. Development of Crypto Applications with high level security.

Methods and systems with high security level have been developed for the synthesis of cryptographic algorithms with modified S-boxes for standard algorithms such as the AES, true random – pseudo random number generators and devices of error control for real time communication systems. Security conscious businesses and organizations may use open source Crypto Applications with high level security, in order to maintain data integrity and security. The aim is to exclude the possibility of unauthorized access by government agencies, the initial algorithm designers and hackers. The laboratory has already provided users and Telecommunications, e commerce and e banking organizations with crypto tools for their exclusive use.

- 3. Development of Power Analysis attacks resilient AES implementations.

Power analysis attacks threat a large number of simple computer users as, currently, 60% of the computer terminals include embedded microcontrollers and smart cards. Such an attack may expose the closed elements (keys and access codes) of the network protocols for data security.

The i-Lab has developed techniques for the polymorphic implementation of AES algorithm on microcontrollers and smart-cards.



Picture 1. Platform for develop and testing polymorphic AES implementations

The techniques for polymorphic implementation have been implemented on small microcontrollers that are suitable for embedded operation.

- 4. Development identification systems for large number of users for high level security

A particularly acute problem, is the problem of fast and secure identification in mobile devices and embedded microcontrollers, with limited energy consumption possibilities, that are commonly end user devices.

The i-Lab developed algorithms that accelerate «zero knowledge» user identification via hardware implementations. They are based on using finite field arithmetic to replace the usual modular arithmetic. This solution has facilitated the development and provision of innovative remote services with strong user authentication, but without the need for physical evidence.

- 5. Processing methods for Information Availability using Cloud Technologies

A pre-requisite in order to guarantee the high reliability of information storage in distributed systems, is the existence of effective means for recovering data in the case of loss of access to one or more storage nodes.

The i-Lab developed method for backup and restoring data that is stored on different remote disks. The method is highly resilient to temporary or permanent loss of access to a significant proportion of these nodes. The proposed method ensures a high level of survivability of cloud systems in demanding applications.

- 6. Development and processing methods for authenticating users and the fast computation of PKI on Cloud Technologies

The emergence and increasing use of cloud technologies affect the security of computer information processing. Additionally, the availability of powerful computing resources may allow potential attackers to multiply the effectiveness of overcoming existing information security systems.

The i-Lab developed methods for securely performing the calculations required for modular exponentiation, an operation fundamental to many cryptographic algorithms, using remote or distant computational resources. These methods avoid the disclosure to the cloud resource, of either the data or the secret keys.

CONCLUSIONS

A number of technological advances have been prevented that provide tailored, modified or targeted solutions to common data security, integrity and reliability problems. These advances promote the ability of technology users to incorporate cutting edge information protection into innovative applications. Several of these techniques are already being applied by financial institutions, industries and government agencies, while the remaining have been developed as operational prototypes. The Informatics Lab of the Hellenic Military Academy is an active research and teaching institution, presenting a diverse set of specializations and a highly successful history of National and International collaborations.

Picture 2. Security algorithms for identification and error control incorporated in Arduino controlled drone

КРИПТОГРАФИЧЕСКИЙ АПОКАЛИПСИС VS ПОСТКВАНТОВЫЙ МИР

Почти детективная история о постквантовой криптографии.

Александр ПОТИЙ

Профессор
Заместитель главного конструктора ЗАО «Институт Информационных Технологий»

ВАШИНГТОН, 26 МАЯ 201X. 3.15

Генерал Т.А. проснулся от резкого звонка. Он протянул руку к телефону и, мельком взглянув на часы, автоматически запомнил время. Звонил дежурный офицер, который коротко доложил:

– Сэр, докладывает дежурный офицер Джонсон. Код «Квант». Дежурная машина уже в пути.

– Спасибо, Джонсон. – ответил генерал и дал отбой.

Генерал ждал этого кода, но не так скоро.

– Неужели началось? – подумал он.

Машина прибыла через 15 минут. Этого было вполне достаточно, чтобы собраться и выехать в штаб-квартиру Агентства. Дорога заняла не очень много времени...

ШТАБ-КВАРТИРА АГЕНТСТВА. 4:00

Удобно разместившись за рабочим столом, генерал выслушал доклад дежурного офицера. Да, это случилось. Дежурный офицер доложил, что в 3.05 ему поступил звонок из Центра мониторинга, из которого стало ясно, что совместный канадско-японский эксперимент по испытанию так называемого large-scale квантового компьютера увенчался успехом. Центр мониторинга Агентства давно отслеживал каналы коммуникации ученых, работающих в этом проекта, и сегодня из их переговоров стало ясно, что этот компьютер создан.

У Агентства был и свой интерес. В подвале, там, где раньше стоял знаменитый CRAY, уже работал квантовый вычислитель. Генерал поблагодарил офицера и дал ему указания по началу действий, в соответствии с кодом «Квант». Машина завертелась, и через 20 минут в кабинете генерала должны были собраться сотрудники, ответственные за окончательное уточнение плана действий на случай «криптографического апокалипсиса». Генерал слегка улыбнулся про себя, не думал он, что так скоро придется реально рассматривать такой сценарий. Офицер ушел, прикрыв дверь. У генерала было 20 минут до начала совещания, и он решил просмотреть некоторые свои материалы и освежить память.

Он достал папку из ящика стола и открыл ее. Первым документом была короткая справка по отчету[1] N8 технического комитета Quantum-Safe Cryptography (QSC, https://portal.etsi.org/tb.aspx?tbid=836&SubTB=836). Это комитет был создан ETSI (European Telecommunications Standards Institute) для разработки предложений и стандартизации решений так называемой

[1] Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

TABLE 1

COMPARISON OF CONVERTIONAL AND QUANTUM SECURITY LEVELS OF SOME POPULAF CIPHERS

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

квантово-безопасной криптографии. На первой же странице этого отчета специалисты в 2015 году утверждали что: «Без квантово-безопасной криптографии любая информация, которая передавалась ранее и будет передаваться в будущем по сетям, является уязвимой к перехвату и раскрытию». В отчете очень ясно были обрисованы угрозы появления квантового компьютера. Перед глазами генерала лежала простая картинка с тремя вопросами:

X: «how many years we need our encryption to be secure»;

Y: «how many years it will take us to make our IT infrastructure quantum-safe»;

Z: «how many years before a large-scale quantum computer will be built».

«Судя по докладу дежурного офицера, мы ошиблись с прогнозами величины параметра Z. И этот момент наступил намного раньше, чем мы ожидали» – подумал генерал. Что это значило? В справке четко указывалось, что:

1. Любая криптосистема, стойкость которой опиралась на математическую сложность задачи факторизации целого числа и дискретного логарифма, с сегодняшнего дня стала равна нулю. А это включает все RSA, RSA, DSA, DH, ECDH, ECDSA криптосистемы и их многочисленные модификации.

2. Любой криптопротокол, построенный на основе этих криптосистем, с сегодняшнего дня не является безопасным.

3. Любой продукт и система защиты, использующие эти протоколы, с сегодняшнего дня не защищены.

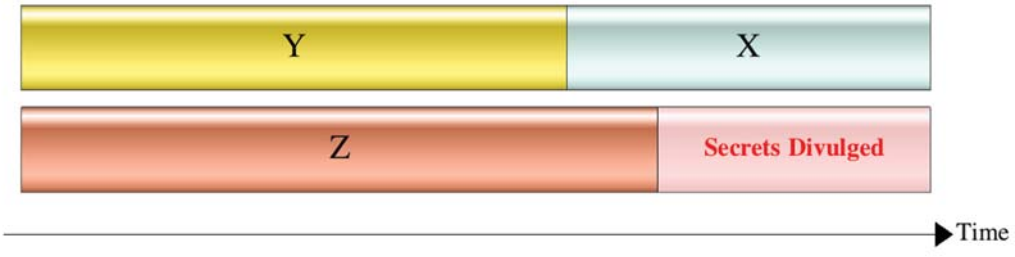
Генерал посмотрел на таблицу, приведенную в отчете: (табл. 1)

Увидев колонки цифр, он еще раз убедился – надеяться можно только на новый блочный шифр AES, который обеспечивает нужную стойкость. Все несимметричные алгоритмы можно смело выбросить.

В следующей справке приводились данные, в каких сферах в первую очередь стоит ожидать проблем. Эти вездесущие RSA и ECC крепко посадили всех на технологический наркотик. Складывалось впечатление, что это была чья-то злая шутка. Инфраструктура открытого ключа, безопасное распределения программного обеспечения, федеративная авторизация, обмен ключами по открытым каналам, защищенная почта S/MIME, VPN и IPSec, SSL и TLS – все теперь под угрозой. Все эти технологии в один момент стали небезопасными. Под угрозой оказались миллиарды оконечных устройств пользователей (генерал вспомнил доклад Bart Preneel[2], в котором он отметил, что различных оконечных устройств и приложений, уязвимых теперь уже в 2014 году, было около 40 миллиардов), вся инфраструктура

РИСУНОК 1

LEAD TIME REQUIRED FOR QUANTUM SAFETY



[2] http://www.etsi.org/images/files/Events/2014/201410_Crypto/e-proceedings-QSC-14.pdf

TABLE 2

SUITE B – RECOMMENDATION NSA

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

шифрования в сетях, облачные хранилища, многочисленные SCADA-системы. И хоть в последних и использовался надежный AES, но распределение ключей строилось на уже небезопасных протоколах.

Его аналитики доложили, что наиболее уязвимыми сферами станут медицина, финансы, мобильные приложения (а это экосистема электронной идентификации, защита авторских прав на цифровой контент, удаленное управления бизнес-процессами, облачные сервисы). На четвертом месте стоял Интернет вещей и смарт-транспорт. На генерала ощутимо повеяло холодком криптографического апокалипсиса, за которым надвигался коллапс страховых компаний, массовая подделка электронной идентичности, управленческий хаос и «бунт» смарт-машин. Словом – крах цифрового мира. Генерал улыбнулся: «Неужели такое возможно!».

Генерал взглянул на часы – подходит время рабочего совещания. Перед глазами уже стояла четкая картинка реальных вызовов, с которым уже утром столкнется мир.

КАБИНЕТ ДИРЕКТОРА АГЕНТСТВА. 4.20

За достаточно просторным столом для совещаний разместилось не так много людей.

– Джентльмены, – начал генерал, – вы все знаете, по какому поводу мы здесь собрались. Наша задача уточнить некоторые моменты и сформулировать конкретные действия, чтобы минимизировать возможные риски. Я уже дал распоряжения начать подготовку всех документов, предусмотренных нашим сценарием. Приступим. Первое, что я хотел бы уточнить, какие мероприятия мы уже провели и есть ли какие либо результаты?

За эти вопросы отвечал отдел анализа криптографических рисков. Его возглавлял молодой выпускник MIT. Он четко и ясно изложил результаты работы Агентства в этом направлении.

Во-первых, он доложил, что еще с 2015 года Агентство совместно с NIST (National Institute of Standards and Technology) на регулярной основе проводят специальные семинары по проблеме постквантовой криптографии (http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm). На этих семинарах, при участии самых видных ученых и специалистов США и других стран в области криптографии и сетевой безопасности, разгорались нешуточные споры. Как результат работы этих семинаров, NIST в феврале 2016 года выпустил отчет NISTIR 8105[3]. В отчете, в частности, был дан краткий обзор так называемой квантово-устойчивой криптографии (Quantum-Resistant Cryptography). NIST уже тогда подтвердил, что существующие в США решения на основе RSA и эллиптических кривых будут уязвимы.

[3] NISTIR 8105 Report on Post – Quantum Cryptography http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf

Второе. Опираясь на эти выводы, Агентство в марте 2016 года выпустило специальный бюллетень, в котором обратилось ко всем крупным вендорам в США поменить с переходом в своих продуктах на использование эллиптических кривых[4]. На время переходного периода Агентство разработала набор требований – Suite B, которым и рекомендуется придерживаться всем компаниям при использовании криптографических алгоритмов (табл. 2).

В-третьих, NIST сформировал группу и организовал работы в рамках Post-Quantum crypto Project. Задача – в течение трех-пяти лет разработать и утвердить новые стандарты, которые будут удовлетворять требованиям стойкости к квантовым вычислениям.

«Здесь мы уже опаздываем» – подумал генерал.

– Что на сегодняшний день предлагает NIST? – задал вопрос генерал.

– На сегодняшний день – докладывал начальник отдела, – они предлагают сконцентрировать усилия в нескольких направлениях.

Начальник отдела показал небольшую таблицу (табл. 3).

– Однако на сегодняшний день мы не имеем в своем распоряжении какого-либо эффективного, доверенного и удобного для реализации криптоалгоритма, – закончил свой доклад начальник отдела.

– Так, – не без сарказма спросил генерал, – а что наши европейские и другие друзья? Как они подготовились к этому «чудесному» утру?

На этот раз докладывал начальник управления по международным связям. В докладе он отметил, что коллеги из Евросоюза двигаются примерно в этом же направлении.

С 2013 года ETSI начал проводить регулярные семинары по вопросам квантово-безопасной криптографии (quantum-safe cryptography) и уже провел три таких семинара[5]. Последний был в сентябре 2016 года. Было решено взять этот термин для обозначения такого класса криптоалгоритмов. Япония проводит такие конференции с 2011 года[6]. И это также являлось одним из факторов успеха японских специалистов в разработке квантового компьютера.

После семинара в 2015 году ETSI принял решение и сформировал технический комитет по разработке стандартов постквантовой криптографии – ETSI Quantum-Safe

[4] https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm
[5] http://www.etsi.org/news-events/events/648-crypto-workshop2013
[6] https://pqcrypto2016.jp/

ТАБЛИЦА 3

ОСНОВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЯ ПОСТКВАНТОВОЙ КРИПТОГРАФИИ

Lattice -based cryptography	Cryptosystems based on lattice problems have received renewed interest, for a few reasons. Exciting new applications (such as fully homomorphic encryption, code obfuscation, and attribute -based encryption) have been made possible using lattice-based cryptography. Most lattice-based key establishment algorithms are relatively simple, efficient, and highly parallelizable. Also, the security of some lattice -based systems are provably secure under a worst -case hardness assumption, rather than on the average case. On the other hand, it has proven difficult to give precise estimates of the security of lattice schemes against even known cryptanalysis techniques.
Code - based cryptography	In 1978, the McEliece cryptosystem was first proposed, and has not been broken since. Since that time, other systems based on error-correcting codes have been proposed. While quite fast, most code -based primitives suffer from having very large key sizes. Newer variants have introduced more structure into the codes in an attempt to reduce the key sizes, however the added structure has also led to successful attacks on some proposals. While there have been some proposals for code-based signature s, code-based cryptography has seen more success with encryption schemes.
Multivariate polynomial cryptography	These schemes are based on the difficulty of solving systems of multivariate polynomials over finite fields. Several multivariate cryptosystems have been proposed over the past few decades, with many having been broken While there have been some proposals for multivariate encryption schemes , multivariate cryptography has historically been more successful as an approach to signatures.
Hash - based signatures	Hash-based signatures are digital signatures constructed using hash functions. Their security, even against quantum attacks, is well understood. Many of the more efficient hash-based signature schemes have the drawback that the signer must keep a record of the exact number of previously signed messages, and any error in this record will result in insecurity. Another drawback is that they can produce only a limited number of signatures. The number of signatures can be increased, even to the point of being effectively unlimited, but this also increases the signature size.

Cryptography (QSC) Industry Specification Group (ISG)[7]. В июне 2015 года этот комитет подготовил белую книгу, в которой подробно изложены проблемы и вызовы для криптографии в посквантовый период[8].

Нужно отметить, что европейский союз решил объединить финансовые усилия для решения этой проблемы и в рамках глобальной европейской программы HORIZON2020 начал осуществлять финансирование теоретических и практических работ в области постквантовой криптографии консорциума ведущих европейских университетов и промышленных компаний.

– По сути, у них сейчас работают в этом направлении и органы стандартизации и наиболее мощные университеты и промышленные компании, – отметил офицер.

– И какие у них результаты? – задал вопрос генерал.

– На сегодняшний день они провели определенный анализ возможных решений, а также сделали некоторые их оценки. Некоторые результаты я уже докладывал Вам, – ответил офицер. – В последнем руководстве ETSI[9] они предлагают провести анализ различных предложений в направлениях, которые также рекомендует NIST (табл. 4)

– Постойте, – остановил генерал офицера, – в последней строке я вижу изогении.

– Да, сэр. Европейские коллеги считают, что с эллиптическими кривыми еще можно поработать.

– Кто еще так считает? – спросил генерал.

– По нашим сведениям, такого же мнения придерживается одна небольшая группа украинских криптографов.

– Мы их знаем?

– Не очень, сэр. Удивительные люди. При таком финансировании упорно работают и продолжают поддерживать украинскую систему криптозащиты на плаву. Они даже приняли свои национальные стандарты[10,11], которые могут быть устойчивыми к квантовым вычислениям.

«Нужно будет позже получше познакомиться с работами этой группы» – подумал генерал.

– Продолжайте.

– Да, сэр. Как я уже отметил, европейцы также пока не имеют приемлемого решения по постквантовым алгоритмам.

[7] http://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography

[8] Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

[9] ETSI EG 203 310 (2016-04) CYBER: Post Quantum Computing Impact on ICT System; Recommendations on Business Continuity and Algorithm selection

[10] Національний стандарт України ДСТУ 7624:2014. Симетричний блоковий шифр.

[11] Національний стандарт України ДСТУ 7564:2014. Геш-функція.

ТАБЛИЦА 4

РАЗМЕРЫ КЛЮЧЕЙ ВОЗМОЖНЫХ КАНДИДАТОВ НА ПОСТКВАНТОВЫЕ АЛГОРИТМЫ

Type	Scheme	Security	Public key	Signature
Lattice	Lyubashevsky	–	1 664 bytes	2 560 bytes
	NTRU-MLS	128 bits	988 bytes	988 bytes
	Aguilar et al	128 bits	1 082 bytes	1 894 bytes
	Cüneysu et al	80 bits	1 472 bytes	1 120 bytes
	BLISS	128 bits	896 bytes	640 bytes
	Ducas et al	80 bits	320 bytes	320 bytes
	HIMMO	128 bits	32 bytes	–
MQ	Quartz	80 bits	72 237 bytes	16 bytes
	Ding	123 bits	142 576 bytes	21 bytes
	UOV	128 bits	413 145 bytes	135 bytes
	Cyclic-UOV	128 bits	60 840 bytes	135 bytes
	Rainbow	128 bits	139 363 bytes	79 bytes
	Cyclic-Raibow	128 bits	48 411 bytes	79 bytes
Code	Parallel-CFS	120 bits	503 316 480 bytes	108 bytes
	Cayrel et al	128 bits	10 920 bytes	47 248 bytes
	Cyclic-Cayrel et al	128 bits	208 bytes	47 248 bytes
	RankSing	130 bits	7 200 bytes	1 080 bytes
	Cyclic- RankSing	130 bits	3 538 bytes	1 080 bytes
Hash	Merkle	128 bits	32 bytes	1 731 bytes
	Leighton-Micali	128 bits	20 bytes	668 bytes
	XMSS	256 bits	64 bytes	8 392 bytes
	SPHINCS	256 bits	1 056 bytes	41 000 bytes
Isogeny	Jao-Soukharev	128 bits	768 bytes	1 280 bytes
	Sun-Tian-Wang	128 bits	768 bytes	16 bytes

ТАБЛИЦА 5

РЕКОМЕНДАЦИИ ETSI

Field	Recommendations
Symmetric encryption	AES – 256; Salsa20 – 256; Serpent 256.
Symmetric authentication	GCM 96 bit none, 128 bit authenticator; Poly 1305.
Public-key encryption	McEliece with binary Goppa code n=6960; k=5413; t=119 errors; Quasi-cycle MDPC code n=2^16+6; k=2^15+3; d=274; t=264; NTRU.
Public-key signature	XMSS; SPHINCS-256; HFEv.

На данный момент они придерживаются рекомендаций 2015 года (табл. 5).

Свои рекомендации также сформировала и ENISA (Европейское агентство по сетевой безопасности) (рис 2).[12]

– Выводы, офицер. – коротко сказал генерал.

– Сэр, по нашему мнению, сегодняшняя ситуация европейцев также застанет врасплох.

В комнате для совещания наступила тишина. Собственно заслушивать кого-либо еще нужды не было. Действительно, ситуация застала врасплох. Никто не ожидал, что успех в построении квантового компьютера произойдете так быстро. Но таковы реалии мира глобальных технологий. «Эффект синергии» – вспомнил генерал высказывание одного профессора на конференции по резильентным технологиям.

– Что ж, джентельмены. Ситуация действительно не очень приятная. – начал генерал. В комнату зашел дежурный офицер и доложил генералу о том, что первые мероприятия по сценарию «Квант» уже выполнены.

– Хорошо, – ответил генерал. – Господа, все же мы были готовы к развитию событий. Мне доложили, что основные распоряжения уже переданы. Уже сейчас осуществляется оперативный переход на новые ключи в вооруженных сила и других ведомствах, которые были ранее доставлены классическим способом – в конвертах. С сегодняшнего дня обмен ключами по открытым каналам будет запрещен. Пресс службу прошу подготовить пресс релиз для гражданских ведомств. Оперативными вопросами уже занимаются. Так что я не думаю, что завтра утром наступит криптографический апокалипсис, мы к этому подготовились.

Нам же необходимо заняться следующим.

РИСУНОК 2

РЕКОМЕНДАЦИИ ENISA

Good	Bad
Authenticated encryption	Encryption only, e.g. AES-CBC
– AES-CMM	RC4, A5/2, E0, DST, Keeloq, Crypto-1, Hitag-2, DSAA, DSC, GMR-1, GMR-2, CSS
– HC-128 + Poly1305	MD2, MD4, MD5, SHA-1
HMAC-SHA-2	RSA PKCS#1 v.5
SHA-3	DSA, ECDSA
Diffie-Hellman	Dual_EC_DRBG
– $Z_p \geq 2048$	ECC curves from NIST
– ECC $\geq$ 256 and up	SSL 3.0
ECIES $\geq$ 256 and up	TLS with RSA key exchange
RSA KEM-DEM $\geq$ 2048	Skype
	Implementations that do not run in constant time

Перед нами стоят три важные задачи:

Первое – создать эффективный криптоалгоритм, противостоящий квантовым вызовам. Нам нужно дать ответ, почему мы просто не можем увеличить объем ключей в уже существующих алгоритмах и сформулировать четкие показатели эффективности новых алгоритмов.

Второе – сформировать необходимый уровень уверенности, гарантий и уверенности в новых алгоритмах. Это сложная задача. Думаю, она может быть решена только через максимальную открытость их разработки с привлечением широкого круга специалистов и аналитиков.

Третье – нам нужно создать удобный алгоритм и криптографические устройства. Никто не будет сегодня бегать с запечатанными конвертами или встраивать новые громадные железки. И это тоже важная задача.

И самое главное – на это все у нас очень мало времени.

Итак, господа, добро пожаловать в постквантовый мир!!

[12] http://www.enisa.europa.eu/activi ties/identity-and-trust/ library/deliverables/algorithms-key-sizes-and-parameters-report

СТОИМОСТЬ ПОДПИСКИ В 2016 г.

Для подписчиков из Украины:
- годовая (6 ном.) – 1630 грн. (без НДС);
- полугодовая (3 ном.) – 850 грн. (без НДС)

Для подписчиков из других стран:
- годовая (6 ном.) – 230 евро (без НДС);
- полугодовая (3 ном.) – 120 евро (без НДС)

Оплата в гривнах по курсу НБУ на день платежа.

В стоимость подписки входит доставка Укрпочтой.

Стоимость доставки курьерскими службами необходимо оговаривать с редакцией.

ПОДПИСКА НА ЖУРНАЛ ЧЕРЕЗ АГЕНТСТВА:

в Украине

Укрпочта подписной индекс 23741	
Саммит	+38 044 521 4050
Идея	+38 044 417 8767, 204 3634
Фирма «Периодика»	+38 044 278 0024, 278 6165
KSS	+38 044 585 8080
Меркурий	+38 056 374 90 43, 374 90 55

в России

Каталог «Газеты. Журналы» – подписной индекс 23741

в Латвии, Литве, Эстонии и странах ЕС

Подписное агентство PKS	Тел/факс +371 67509-742
г. Рига, тел. +371 67320-148	
e-mail media@apollo.lv, www.pressa.lv	

ПОДПИСКА НА ЭЛЕКТРОННУЮ ВЕРСИЮ ЖУРНАЛА (PDF-файл)

Для подписчиков из Украины:
- годовая (6 ном.) – 1090 грн. (без НДС);
- полугодовая (3 ном.) – 650 грн. (без НДС)

Для подписчиков из других стран:
- годовая (6 ном.) – 160 евро (без НДС);
- полугодовая (3 ном.) – 90 евро (без НДС)

Оплата в гривнах по курсу НБУ на день платежа.

Подписаться на электронную версию журнала «Карт Бланш» можно на портале **PressPoint** – новой электронной библиотеки печатной периодики. Более подробную информацию можно узнать по линку **http://presspoint.ua**

РЕКЛАМА В НОМЕРЕ

Подписаться с любого номера можно через редакцию:
Тел.: +380 44 248 0 416,
тел. моб.: +380 50 334 7458

E-mail:
Elena@smart-payments.info

ПЕРИОДИЧНОСТЬ ВЫХОДА ЖУРНАЛА

Журнал Карт Бланш выходит 4 раза в году.

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

Редакция журнала принимает технические, информационные, аналитические и другие материалы по вопросам и проблемам развития рынка информационных технологий, инноваций, R&D, а также финтеха, науки и образования и другим актуальным темам в Украине и за рубежом.

КОНФЕРЕНЦІЯ

ПРАВО І ФІНАНСИ
в цифрову епоху

23.06.2016, Київ

ТЕМИ:

Електронна демократія:
важіль для укріплення демократичних принципів суспільства

Право в цифрову епоху:
парадигма балансу та гнучкості

Фінансова безпека України в сучасних умовах

МІСЦЕ ПРОВЕДЕННЯ:

Конференц-зал
Київського національного університету технології і дизайну
м. Київ, вул. Немировича-Данченка

Тел.: +38 (095) 356-99-69; +38(067) 375-76-37
E-mail: marina.medinskaya@it-alliance.org.ua oksana.hahina@it-alliance.org.ua

CONTEMPORARY PLASTIC CARD BANKING TECHNOLOGIES PROVIDER

VISA MasterCard

HIGH-QUALITY and FLEXIBLE CARD SOLUTIONS
FOR BANKS and MOBILE OPERATORS
FROM A CERTIFIED MANUFACTURER
FROM EASTERN EUROPE

SALES OFFICE:
Nyzhneyurkivska Str., 45-A
04080 Kyiv, Ukraine
Phone/fax: +38044 425-87-87
e-mail: sales@plasticcard.kiev.ua

www.plasticcard.kiev.ua

Plastic Card

production of any types of cards
personalization & packaging
software development