ВЫСОКИЕ ТЕХНОЛОГИИ И БЕЗОПАСНОСТЬ

М.Макушин

Можно понять правительство, когда оно экономит на социальных сферах государства. Нельзя понять, но можно объяснить, почему не предпринимается ничего для развития высокотехнологических отраслей экономики страны. Но если средства экономятся на безопасности граждан, этого ни понять, ни объяснить невозможно ничем, кроме как некомпетентностью. Президент может сколь угодно долго говорить о войне с терроризмом, но чего стоят его слова, если они не подкреплены реальными действиями? А сегодня обеспечение безопасности во многом – вопрос развития технологий, прежде всего электронных. Чтобы оценить ситуацию в этой области в России, уместно сравнить ее с другими странами.

ВМЕСТО ПРЕДИСЛОВИЯ

За прошедшее с 11 сентября 2001 года время во всем мире активно предпринимались усилия по поиску путей обеспечения безопасности авиапассажиров, выявлению террористов, ядовитых и взрывчатых веществ, оружия и наркотиков на границах, пунктах пропуска и т.п. Но в России августовские взрывы самолетов и бесланская трагедия в очередной раз показали, что чужие уроки не пошли нам впрок. Как главное наше достижение, по телевизору демонстрируют усиление личного досмотра в аэропортах. И при этом никто не говорит о выделении средств на разработку и внедрение технологий обеспечения безопасности нового поколения. Кто и как может решить эти задачи?

Разумеется, прежде всего целесообразно обратить взор на высокотехнологичный сектор оборонно-промышленного комплекса России. Но задача ведь не только в том, чтобы создать что-то подходящее, но и в том, чтобы производить это в достаточных объемах по приемлемым ценам. Во всех странах высокотехнологичные отрасли промышленности являются объектом пристального внимания и заботы властей, защищающих их интересы. Для поддержки наиболее значимых направлений передовые страны используют такие надежные инструменты, как таможенные тарифы, квотирование и антидемпинговые процедуры. В эпоху ВТО для национальных экономик все большее значение приобретают финансирование НИОКР, помощь частной промышленности в освоении их результатов, предоставление налоговых скидок на НИОКР, приобретение и освоение нового оборудования и технологий, ускоренная амортизация и другие льготы, вплоть до прямого финансирования конкретных проектов [1].

В России же "реформаторы" уже больше десятилетия повторяют давно протухшие заклинания, что "...рынок все сам отрегулирует", уничтожая при этом целые отрасли. Бешенные прибыли от нефтедолларов не просто собираются в "стабилизационном фонде", а вкладываются в ценные бумаги других стран, причем с большим риском и меньшей перспективой, чем это было бы при их вложении в развитие собственных высоких технологий, которые задыхаются от нехватки средств и отсутствия реального стимулирования их деятельности. Этот факт лишний раз подтверждает предательство "экономическим блоком" правительства интересов национальной безопасности России.

ЧТО ДЕЛАЮТ НА ДИКОМ ЗАПАДЕ?

Для решения проблем безопасности государственные структуры зарубежных стран в тесном взаимодействии с национальными разработчиками и производителями активно развивают существующие и осваивают новые технологии, в первую очередь наноэлектронные. Для обзора ситуации в традиционных технологиях достаточно рассмотреть несколько примеров из области оптических систем, средств сканирования, детекторов, которые уже нашли применение на практике.

Сразу после событий 11 сентября 2001 года начались интенсивные разработки новых оптических систем безопасности для предотвращения террористических актов на воздушном транспорте. Сложность задачи в том, что не все взрывчатые вещества (ВВ) могут быть обнаружены при помощи рентгеновского оборудования. Совместными усилиями Федерального управления авиации США, канадских фирм Transport Canada и Intelligent Detection Systems разработан новый метод обнаружения следов ВВ на внешней поверхности багажа при помощи лазерного излучения [2].

Известно, что после упаковки ВВ в чемодан на его внешних частях остаются микроскопические следы этого вещества. Обычные методы обнаружения, которые заключаются в обработке поверхности чемодана растворителем с последующим исследованием растворенных веществ при помощи газового хроматографа, хотя и отличаются высокой чувствительностью, но предполагают лишь выборочную проверку багажа. Новая лазерная система позволяет сканировать весь багаж. Предложенный метод заключается в исследовании спектра светового импульса, который генерируется при детонации микроскопических частиц взрывчатого вещества под воздействием лазерного излучения.

Используя импульсное излучение CO_2-лазера с длиной волны 10,6 мкм, исследователи показали, что световой импульс, испускаемый при детонации ВВ, фиксируется раньше, чем световой импульс от сахара (типичное невзрывоопасное горючее вещество). Такие ВВ, как PETN (пентрит), RDX (гексоген) и Semex-H детонировали через 1–4 мс после начала воздействия лазерного импульса, в то время как импульс от горящего сахара фиксировался через 7 мс. Было обнаружено, что длинные лазерные импульсы (~1 мс) более эффективны, чем короткие (~1 нс), поскольку последние вызывают ионизацию исследуемого вещества до его детонации. Спектры излучения, генерируемого при детонации взрывчатых веществ, также легко идентифи-

цировать и отличить от спектра горения сахара. В процессе сканирования поверхности багажа лазерное излучение фокусируется в пятно диаметром 1 мм. Система реагирует на частицы массой до 1 нг.

Специалисты Тихоокеанской национальной лаборатории США (г. Ричленд, шт. Вашингтон) разработали для аэропортов новую систему сканирования пассажиров, позволяющую обнаруживать спрятанное под одеждой оружие [2]. В системе используется излучение миллиметрового диапазона (30–300 ГГц), а также метод оптической голографии в применении к этой полосе частот. Среди основных достоинств новой системы – возможность обнаруживать предметы под одеждой и высокий коэффициент отражения излучения от поверхностей различных материалов (металла, пластика и др.).

Отмечается, что система первого поколения имела существенные недостатки (малые площадь и глубина резкости изображения). Однако последующие работы показали, что устранить эти недостатки можно, используя широкополосный источник излучения, а также оригинальный алгоритм реконструкции трехмерного изображения с большой глубиной резкости. Этот алгоритм объединил в себе методы оптической голографии и синтезированной апертуры. При лабораторных испытаниях с применением излучения на частоте 27–33 ГГц получены детальные изображения предметов, спрятанных под одеждой человека. Использование излучения с большей частотой позволит получить изображение с разрешением до 3 мм. В этом случае можно обнаружить оружие малых габаритов и отличить его от других безобидных предметов, например таких, как сотовый телефон.

С целью освоения производства новой сканирующей системы на коммерческой основе в конце 2002 года была создана фирма Safeview (г. Ричмонд, шт. Вашингтон). Одним из аспектов работ ее специалистов стало решение вопроса неприкосновенности частной жизни, поскольку оператор сканирующей системы в процессе работы наблюдает изображение раздетого человека. Была разработана специальная программа, преобразующая полученное изображение таким образом, что оператор видит только спрятанные под одеждой предметы.

Ведутся работы и по совершенствованию систем детекторов. Используемые сегодня детекторы оружия реагируют на все металлические предметы – пистолеты, ножи, ключи, металлические застежки на одежде и обуви и т.д., не отличая их друг от друга. Это затрудняет досмотр и приводит к огромным очередям.

Детекторам металлов на основе активных индукционных катушек присущ ряд недостатков: низкая чувствительность, наличие "мертвых зон" обнаружения и малая производительность. Для решения этих проблем разработчики компании View Systems при сотрудничестве с министерствами юстиции и энергетики США создали систему обнаружения скрытого оружия (concealed-weapons-detection – CWD), которая не только выявляет оружие, но и может отличить представляющие угрозу предметы от неопасных (например, пистолет от сотового телефона).

Структурно система CWD использует набор датчиков, размещенных на портале, и ПО на базе нейросетевых алгоритмов для распознавания образов, реализованных на ПК с процессором типа Pentium в среде Windows. Разработчики продемонстрировали возможность выявления местоположения представляющего угрозу объекта в верхней, средней или нижней части человека. Алгоритмы обработки показаний датчиков вычисляют вероятность корреляции собранной сигнатуры с имеющимися в базе данных оружия и других предметов. Испытания системы продемонстрировали, что представляющие угрозу объекты отделяются от неопасных предметов с вероятностью 97,3% [3]. Проводились испытания и по способности идентифицировать различные предметы. Так, лезвие бритвы помещали в нагрудный карман, сотовый телефон – на боку, а нож – в ботинке. Система CWD верно классифицировала предметы в 86% случаев.

Немалую угрозу могут представить и террористические акты с применением биологического оружия. Их призвана предотвращать создаваемая в США обширная сеть обнаружения этой угрозы. Системы для выявления химически и биологически опасных объектов развертываются в аэро- и морских портах, на таможенных и пограничных пунктах, почтамптах и т.д. При этом предпочтение отдается портативному оборудованию.

Недавно Национальный научный фонд США дал зеленый свет созданию портативной системы на основе прототипа комбинированного био- и химического сенсора, разработанного в Университете Буффало. Устройство включает светоизлучающий диод, матрицу на основе ксерогелей с впечатанными протеинами (protein-imprinted xerogels with integrated emission sites) и КМОП-детектор. Ксерогели с впечатанными протеинами наносятся на стеклянную подложку с наноразмерными порами. Матрица содержит эталонные молекулы веществ, подлежащих идентификации, и способна захватить молекулы потенциальных токсинов. Под воздействием излучения светодиода молекулы флюоресцируют, и сравнивая интенсивность флюоресценции с эталоном с помощью КМОП-сенсора, можно определить наличие того или иного токсина [4]. Кроме того, устройство способно определить концентрацию токсина путем измерения интенсивности флюоресценции.

Опытный образец устройства изготавливался по стандартному технологическому процессу с разрешением 1,6 мкм корпорацией Mosis. По оценкам, стоимость самого сенсорного устройства (источник света, матрица и КМОП-детектор) в серийном производстве не должна превышать 50 долларов.

Первоначально данное устройство предназначалось для обнаружения кислорода. Но разработчики заявляют, что разнообразие веществ, которые можно обнаруживать, зависит от только ксерогелевых матриц. Поэтому в ближайших планах – создание основного набора эталонов, который будет включать в себя вещества, наиболее вероятные для использования террористами. Прежде всего – токсины на белковой основе, такие как стафилококк, ботулин и т.п., для которых легко создать шаблон в ксерогеле. Предполагается, что устройства будут оснащены интерфейсом для подключения к КПК и сетям передачи информации для быстрой отправки сообщения о случае обнаружении опасного вещества в соответствующие службы.

О создании и испытании данных систем сообщалось в период с декабря 2002 г. по ноябрь 2003 г. Их окончательная доводка проводилась вплоть до лета 2004 года, и сейчас они достаточно хорошо показывают себя на практике. Помимо описанной системы, в данной области есть еще более десятки разработок как законченных, так и ведущихся. И это только в США.

Так что с раздеваниями и осмотрами каблуков в западных аэропортах достаточно скоро будет покончено. Особенно если учесть работы в области биоидентификации, развертывания системы электронных паспортов с биометрическими данными владельца и т.п.

НАНОТЕХНОЛОГИИ – НА СЛУЖБЕ БЕЗОПАСНОСТИ

Исследования в области нанотехнологий ведутся по трем основным направлениям: биология, медицина и микроэлектроника. Значительная часть зарубежных исследований носит военный характер [5]. Современные разработки микроматриц нанодатчиков и "нанолабораторий на кристалле" открывают перспективу создания малогабаритных комплексов, размером от сотового телефона до ручного металлодетектора, способных распознавать в реальном времени множество видов взрывчатых и отравляющих веществ, наркотиков и бактериологического оружия. Однако опытных образцов подобных систем, пригод-

ных для промышленного внедрения, еще нет, хотя они и ожидаются в ближайшем будущем.

При этом необходимо отметить, что США, ЕС и Япония тратят на нанотехнологические НИОКР по 700–900 млн. долл. государственных средств ежегодно. Отраслевые частнопромышленные ассоциации также формируют свои программы, координирующиеся с правительственными в целях повышения эффективности работ и избежания дублирования. При этом они также не отказываются от государственной помощи. Правда, их объемы инвестиций пока на порядок меньше государственных, но по мере коммерческого освоения нанотехнологий ситуация будет меняться. Примечательно, что парламент Великобритании весной 2004 года обвинил свое правительство в тупости за недостаточное финансирование программ в области нанотехнологии – там объемы инвестиций в это направление составляют порядка 90 млн. долл. (см. врезку).

Интересно, что сказал бы британский парламент о политике нашего правительства в этой области? Отдельной нанопрограммы в России нет, а те крохи, которые теоретически могут быть выделены на подобные исследования в рамках ФЦП "Национальная технологическая база", отстают от британских порядка на два...

У НАС ОПЯТЬ НЕТ ДЕНЕГ...

Есть ли у нас перспективные разработки в области систем безопасности, аналогичные западным? Да, работы в области газоанализаторов в СССР и даже в нынешней России находятся на достаточно приемлемом по мировым меркам уровне. На уровне единичных приборов и опытных образцов у нас имеются разработки в области оптического газоанализа, спектрлюминесценции, электронной и протонной спектрометрии и т.п. Но... Во-первых, у нас опять нет денег... Это было лейтмотивом комментариев после гибели пассажирских самолетов. Правда, в новом бюджете заложено увеличение ассигнований на безопасность и антитеррористические меры. Но достанутся ли они эоектронным предприятиям? Во-вторых, государство уделяет внимание только оборонной и специальной электронике, отдав на откуп иностранным поставщикам рынок электроники гражданской. А это – позиция страуса. На мировом рынке электронных компонентов на военно-ориентированные изделия сейчас приходится менее 2% продаж. Устойчива тенденция использования ИС гражданского назначения в военных и специальных системах, не подвергающихся воздействию радиации, перепадов температуры и резких сотрясений. Этим достигается повышение производительности систем и их удешевление. Многие зарубежные производители комплектующих, начав в качестве военных подрядчиков, в дальнейшем "раскрутились" до транснациональных корпораций именно за счет гражданской продукции. Более того, часть получаемых от этого средств идет и на поддержку исследований в оборонной сфере. Все это возможно благодаря системам стимулирования сектора высоких технологий, существующим в каждой технологически высокоразвитой стране.

Если брать США, то это налоговая скидка порядка 80% на бюджеты НИОКР (из расчета 20% на валовые отчисления последних четырех лет), фактически 50%-ная скидка при коммерциализации технологий, разработанных в национальных (государственных) научно-исследовательских лабораториях (за счет создания СП для доведения этих результатов до уровня коммерческой пригодности, при этом государство вносит свой вклад как деньгами, так и интеллектуальной собственностью – этими самыми результатами). Амортизация основных средств и комплексов производственной и научно-исследовательской техники сокращена до 3–5 лет, что является мощным средством поддержки конкурентоспособности и стимулирования обновления парка различного оборудования. Продолжать можно долго.

О СТРАТЕГИИ РАЗВИТИЯ НАНОТЕХНОЛОГИЙ НА АЛЬБИОНЕ БРИТАНСКОЕ ПРАВИТЕЛЬСТВО ОБВИНЯЕТСЯ В ТУПОСТИ

Парламент Великобритании обвиняет правительство в недофинансировании нанотехнологий, игнорировании советов британских экспертов по созданию как минимум двух нанотехнологических центров и проведении "тупой" политики распределения выделенных на данную тематику средств. В отчете (весна 2004 г.) комитета по науке и технике палаты общин сказано, что министерство торговли и промышленности демонстрирует "робкое и плохое понимание" необходимости работать в соответствии с рекомендациями консультативной группы по мерам капитализации нанотехнологичных НИОКР в стране.

В самом деле, в 2003 году на поддержку микро- и нанотехнологичных производственных инициатив было выделено 165 млн. евро (90 млн. ф.ст.). Микротехнология характеризуется кремниевыми МЭМС, уже имеющими хорошее коммерческое применение. В то же время, нанотехнологии требуют долгосрочного финансирования. Комитет также заявил, что решение правительства выделять средства на эту программу через управления регионального развития является "тупой" стратегией, которая безуспешно пытается примирить конфликт между долгосрочными интересами развития науки и инновационной политики с одной стороны, и краткосрочными интересами развития регионов – с другой. Кроме того, отмечено, что министерство не сумело наладить эффективное взаимодействие академической науки и деловых кругов в данной сфере, что существенно затрудняет развитие нанотехнологий в Великобритании.

На все аспекты нанотехнологий в Великобритании в год выделяется максимум 92 млн. долл. (50 млн. ф.ст.), что составляет менее 1/10 от объемов аналогичных ассигнований в США и Японии, где в течение уже многих лет осуществляются достаточно сложные программы.

По материалам H. Yeates. U.K. Govt Accused of Muddled Nano Strategy. – Electronics Weekly, 4/9/2004.

А что имеем мы? Плата за землю с научно-исследовательских учреждений взимается меньшая, чем с объектов промышленности; научно-исследовательские организации не платят НДС (20%) с федеральных ассигнований на НИОКР (промышленность платит). И это стимулирование?

В заключение отметим, что последние 13 лет в плане развития высоких технологий практически потеряны. А конкуренты уходят все дальше. В результате одним из следствий научно-технической политики, проводимой руководством страны последние 13 лет, стала сама возможность проведения диверсий и на транспорте, и в школах, и в подземных переходах, и на стадионах...

ЛИТЕРАТУРА

1. **Макушин М.** Государство и полупроводниковая промышленность – заботливый опекун курочки Рябы (зарубежный опыт). – Электроника: НТБ, 2002, №6, с. 60–65.
2. **E.Learner.** Photonics promises improved security. – Laser Focus World, December 2002, Volume 38, Issue 12.
3. **P.Reep.** Sharpening the tools of threat detection. – Laser Focus World, April 2003, Volume 39, Issue 4.
4. **R.Colin Johnson.** Biosensor funded for terror war. – www.eetimes.com/at/news/OEG20031112S0034
5. **Макушин М.** Становление многорукого бога (обзор финансирования работ по нанотехнологии). – Электроника: НТБ, 2003, №4, с. 70–74.