

Перспективы развития систем национальной безопасности на основе биометрии

Ю. В. Крылова,

аспирант кафедры экономической теории,
экономический факультет

Санкт-Петербургского государственного университета



Статья посвящена описанию и анализу перспектив развития национальных систем безопасности на основе биометрии. Автор рассматривает новые биометрические технологии, разработанные российской инновационной компанией «Элсис». Биометрическая система безопасности, разработанная «Элсис», была награждена золотой медалью с отличием на Всемирной выставке изобретений и инноваций «Брюссель-Эврика 2001». Применение данных технологий разнообразно: для медицинских целей, для целей идентификации и обеспечения безопасности. Они могут быть использованы для разработки проекта национальной безопасности. Биометрия может стать реальным барьером на пути терроризма. Обеспечение международных аэропортов биометрическими системами безопасности сделало бы невозможным совершение террористических актов, подобных терактам 11 сентября в США.

The article is devoted to a description and analysis of perspectives on the national security systems based on biometrics. The author considers the new biometric technologies developed by the Russian innovative company «Elsys». Biometric Security System and Technology by «Elsys» Corp. was awarded the gold medal with mention on the World Exhibition of Innovation Research and New Technologies «Brussels-Eureka». Applications of these technologies are various with medical, identification and security purposes. They can be used for development of the national security project. Biometrics can be a real barrier on the way of terrorism. Providing the world airports with biometric security systems would make impossible terrorist attacks as the accidents of the 11th of September in the USA.

Ведущие российские экономисты говорят о необходимости разработки новой программы постиндустриализации, ориентированной на достижение конкурентных преимуществ на мировом рынке [1]. В условиях современной России основным конкурентным преимуществом может стать выпуск наукоемкой, технологически сложной продукции, эффективной с точки зрения экспорта, так как она дает возможность получения интеллектуальной ренты. Это тем более важно, так как в России накоплены большие научно-технические заделы. Задача государства заключается в переориентации экономической политики на поддержку приоритетных направлений, с точки зрения стратегических интересов России, с учетом современных мировых тенденций.

Сегодня одним из наиболее перспективных направлений является разработка и производство продукции на основе биотехнологий, например, интеллектуальных систем безопасности на основе биометрии. Биометрические технологии представляют собой технологии XXI в. Они основаны на интеграции исследований в области элект-

роники, информатики, медицины, собственно биометрии. Взаимопроникновение этих наук порождает новые возможности для создания принципиально новых, уникальных товаров и услуг. В соответствии с прогнозами ведущих представителей научно-технической общественности, рынок продукции по данным направлениям исследований будет неуклонно возрастать, что позволит создать уникальную электронную продукцию на основе биотехнологий. Неслучайно, предвидя бурное развитие этого направления, программные документы технологической политики промышленно развитых стран (ПРС) придают большое значение разработке электронной продукции следующего поколения.

Современная биометрия началась с применений в целях контроля доступа на секретные объекты в середине 70-х годов XX в. Биометрические системы идентификации, доступные в настоящее время или находящиеся в стадии разработки, включают в себя системы доступа по отпечатку пальца, ДНК, форме уха, геометрии лица, температуре кожи, отпечатку ладони, сетчатке, радужной оболочке глаза,

подписи и голосу. Сегодня на Западе существует несколько тысяч компьютеризированных мест, хранилищ, исследовательских лабораторий, банков крови, банкоматов, военных сооружений, доступ к которым контролируется устройствами, которые сканируют уникальные характеристики человека. Наряду с функцией идентификации, такие системы имеют ряд других функций, например, учет и контроль рабочего времени, пересечения границ и т.д. В соответствии с ростом числа приложений, где возможно применение биометрических технологий, растет и объем производства биометрических устройств.

Биометрия активно развивается, системы контроля доступа — это, по сути, вчерашний день. Огромный потенциал в биометрии представляет развитие систем безопасности на ее основе, представляющих оптимальное решение данной проблемы.

Касательно российских предприятий электронной индустрии, можно сказать, что здесь накоплен громадный инновационный потенциал, но на сегодняшний день существуют серьезные проблемы внедрения инноваций. Для иллюстрации эффективных российских разработок в сфере биотехнологий приведем конкретные примеры. В данной области представляют интерес разработки интеллектуальных электронных систем национальной безопасности на основе биометрии, предложенные компанией ООО «МП «Элсис» (Санкт-Петербург), имеющей большой опыт в производстве новой электронной продукции.

Рассмотрим более подробно две перспективные, с нашей точки зрения, технологии, подкрепленные наличием патентов [2].

1 Уникальная технология Vibroimage (Аура) позволяет использовать обработку изображений биологических объектов, полученных с помощью обычных видеокамер, для анализа физиологического и нервно-психологического состояния человека. В ходе анализа выявляются состояния агрессии, страха, которые регистрируются в цифровом виде. Практическое применение таких систем достаточно широко как в области медицины (физиологическое состояние человека), так и в области обеспечения безопасности (выявление субъектов, представляющих угрозу для общества вследствие агрессии).

2 Уникальная технология 3D-pulse (объемный пульс) представляет собой возможность с помощью дактилоскопического сенсора получать объемные изменения пульсовой волны для расчета физиологических и нервно-психологических характеристик человека. Технология дает уникальные

возможности: во-первых, возможность дактилоскопической идентификации пользователя, во-вторых, при совмещении с детектором лжи эта технология значительно расширяет его возможности по качественным и временным параметрам. Если рассмотреть это в упрощенном виде, то при демонстрации субъекту ряда визуальных объектов (фотографии террористических актов, например, в случае обеспечения безопасности) или звуковым контакте пульсовая волна будет иметь некоторые особенности при различном отношении субъекта анализа к демонстрируемому или озвученному объекту. На этой основе можно говорить о возможности контролировать не поступки, а мысли и намерения человека, выявляя его потенциальную опасность.

На основе этих технологий разрабатываются системы национальной безопасности, которые имеют большое коммерческое применение, особенно с учетом современных тенденций. Установка таких систем может происходить повсеместно: на стратегически важных, секретных, охраняемых объектах для защиты от несанкционированного доступа и нападений, в аэропортах, таможенных, пограничных пунктах, местах массового скопления народа для предотвращения возможных общественно опасных действий со стороны агрессивно настроенных субъектов, террактов и т.д.

Кроме уникальной возможности выявления преступников и террористов до совершения ими правонарушений и терактов, к преимуществам системы безопасности, разработанной ООО «МП «Элсис», можно отнести ее относительную экономичность. Вследствие уникальных технологических решений стоимость такой системы в десять раз ниже ведущихся на Западе разработок в данной области, что делает их привлекательными для иностранных государств.

В октябре 2001 г. на Второй Российской Венчурной Ярмарке (организатор — Российская ассоциация венчурного инвестирования и Центр стратегических разработок (ЦСР) «Северо-Запад») [3], проводившейся в Санкт-Петербурге, компания «Элсис» получила приз «За лучшую презентацию». Между тем, в ноябре 2001 г. на Всемирной выставке изобретений и инноваций «Брюссель-Эврика 2001» компания «Элсис» была награждена Золотой медалью с отличием, но уже не за оформление стенда, которое было отмечено соотечественниками ранее, а за разработку концепции безопасности на основе биометрической технологии.

Исследования в области биометрических систем безопасности ведутся в настоящее время во многих странах, особенно активно в США, Израиле в

силу объективных причин. Рынок таких интеллектуальных систем неизбежно будет возрастать в силу тенденций, рассматриваемых ниже.

Современные футурологические исследования приводят к выводам о том, что в XXI в. будет наблюдаться усиление конфронтации различных цивилизаций. Известный американский научный и политический деятель, принимавший активное участие в разработке национальной военной стратегии и доктрины национальной безопасности США, Самюэль Хантингтон в своей книге «Столкновение цивилизаций и преобразование мирового порядка» [4] говорит о неизбежности конфликта цивилизаций, порожденного, прежде всего, их культурными, религиозными различиями, которые, в свою очередь, порождают различия в сфере политики и экономики. Можно оспорить выделение в качестве принципиального отличия цивилизаций культурно-религиозной сферы, но сам факт наличия конфликтов в будущем неоспорим.

Отсюда вытекает следующая тенденция: в связи с распространением международного терроризма озабоченность государств состоянием защиты общества будет неуклонно возрастать. Учитывая вышесказанное, можно сделать вывод о том, что наука и техника XXI в. будут работать над проблемой создания систем безопасности на национальном и международном уровнях, а это повлечет за собой развитие ряда отраслей — электроники, информатики и других. Проекты, разработанные ООО «МП «Элсис», в данном контексте представляют интерес, так как их практическое применение позволит проводить биометрическую профилактику преступлений, заранее выявлять лиц, склонных к насилию и агрессии в отношении общества. Например, оснащение такими системами международных аэропортов сделает невозможным повторение террористических актов сентября 2001 г. в Нью-Йорке.

Конечно, российские и зарубежные спецслужбы располагают необходимыми средствами и известным опытом предотвращения терактов. Но темпы распространения терроризма превышают темпы развития технологий защиты. Необходимы превентивные меры, направленные на пресечение самой возможности преступлений.

Необходимо заметить, что введение систем безопасности повлечет за собой изменения в других областях, очевидна необходимость междисциплинарного сотрудничества таких дисциплин, как: экономика, техника, юриспруденция. В качестве иллюстрации приведем пример. Основной принцип в каноническом законода-

тельстве — возникновение юридической ответственности, связанной с применением санкций, после совершения правонарушения. В уголовном праве преступление — это деяние против общества или личности в активной или пассивной форме. Одним из признаков преступления является его наказуемость. Но в отношении религиозных террористов — «камикадзе», которые осознанно идут на смерть, при этом унося жизни невинных жертв, существующая система наказания теряет свою актуальность, становится просто бессмысленной в силу физической невозможности ее применить. Если говорить о системах биометрической профилактики правонарушений, дающих возможность определять лиц, готовых к совершению общественно-опасных деяний, то система наказания должна предусматривать возможность изоляции таких субъектов с целью пресечения правонарушений и защиты граждан от реальных угроз их жизни и здоровью. С точки зрения терроризма, в системе наказания должен действовать не принцип *ex post factum* (после содеянного), а принцип *ex ante* (предвидение, ожидание) в отношении правонарушений.

Представляется преждевременным говорить о смене парадигм в юриспруденции, можно лишь рассматривать варианты развития данного направления. Но тектонический сдвиг, смена парадигм в науке и технике, создание уникальных интеллектуальных систем безопасности, дающих возможность профилактики преступлений на основе контроля за намерениями людей, несомненно, повлечет за собой ряд изменений в смежных областях [5].

Развитие новых биометрических технологий на базе отечественной электроники может обеспечить несколько преимуществ для России в целом:

1 Возможность обеспечения национальной безопасности страны, выигрышное положение при прогнозируемом столкновении цивилизаций, борьбе за новый мировой порядок.

2 Развитие конкурентоспособных технологий и продукции на их основе, дающих возможность получать при экспорте более высокую интеллектуальную ренту.

3 Развитие смежных с электроникой, информатикой, биометрией отраслей и новых производств.

В условиях современной России, значительно отстающей в научно-технологическом развитии от ПРС, на начальном этапе целесообразно развивать исследования в области коммерчески выгодных технологий. С этой точки зрения, рассмотренные технологии имеют большой коммерческий потен-

циал. Ожидается, что именно в области биотехнологии заложены перспективы развития промышленной индустрии. Огромную роль здесь призвана сыграть интеграция экономических и технологических исследований, развитие программ инвестиционной поддержки разработок в области систем биометрической безопасности.

Особую благодарность автор выражает ведущим специалистам компании ООО «МП «Элсис» за оказание помощи при написании статьи.

Литература

1. В. Т. Рязанов. Экономическое развитие России XIX-XX вв. СПб., 1998. С. 713.
2. Материалы касательно биотехнологий Vibroimage и 3D-pulse предоставлены компанией ООО «МП «Элсис» (Санкт-Петербург).
3. <http://www.elsys.ru>
4. С. Хантингтон. Столкновение цивилизаций и преобразование мирового порядка. // Новая постиндустриальная волна на Западе. Антология. / Под ред. В. Л. Иноземцева, М., 1999. С. 528-557
5. Противники биометрии утверждают, что биометрия — это еще один шаг к обществу тотальной идентификации и контроля каж-

дого гражданина, то есть нарушение гражданских свобод, т.к. любой биокод несет в себе больше информации, чем нужно конкретному устройству (биометрическим сканерам) для проверки контроля доступа. Сеть подобных устройств легко может служить инструментом скрытого наблюдения. Подобные дискуссионные вопросы касательно этической стороны возникают и при рассмотрении таких актуальных сегодня проблем, как: эвтаназия и клонирование. Представляется, что эти вопросы не должны препятствовать научно-техническому развитию, тем более, что проблема национальной безопасности отличается от последних тем, что в настоящее время непосредственно затрагивает интересы каждого индивида.

Инновационный бизнес и кооперация: новые правила старой игры

А. В. Ламанов,
кандидат социологических наук,
президент ФПО «Новые транспортные технологии»,
г. Москва



В статье рассмотрены проблемы кооперации малых и средних инновационных организаций с крупными промышленными предприятиями. Дается интерпретация характера подобных отношений, анализируются перспективы сложившейся в переходный период модели «малое инновационное предприятие — заказчик у большого промышленного предприятия».

The article deals with problems concerning cooperation of small and average innovation organizations with large industrial enterprises. It offers an interpretation of characteristic features of the above cooperation and considers prospects of the «small innovation enterprise — customer of large industrial enterprise» model which was built up during the transitive period.

Взаимоотношения организаций, как и взаимоотношения людей, всегда строятся не просто, будь то «жесткая» конкуренция или «мягкая» кооперация. Более того, именно в кооперационной сфере, где нет черно — белого разделения, они наиболее сложны и противоречивы. Именно слабо формализованная и размытая сфера отношений, неподвластная калькуляции, в конечном итоге, решает успех и неуспех экономических контрактов. Неслучайно интерес к теме проявляют как практики, так и теоретики. При этом налицо гуманизация методов исследования, синтез социальных и экономических подходов.

Традиционно выделяют две базовых кооперационных модели [1]:

- иерархизированную структуру с крупной компанией в центре, которая собирает вокруг себя фирмы меньшего размера;

- партнерство предприятий, близких по размеру.

Первая модель первична для всех типов экономик, в том числе западных. В России в силу слабого развития малого и среднего бизнеса она доминантна по сей день. Даже теоретическое оживление в сфере проблематики кооперации начиналось с осмысления опыта взаимодействия крупных предприятий машиностроения с поставщиками-«сателлитами» [2].

Понятно, что число форм взаимодействия не исчисляется двумя базовыми, существуют промежуточные формы. Об одном таком варианте мы писали ранее, в контексте развития инновационного бизнеса [3]. Модель была названа «перевернутой иерархической», поскольку в ней присутствуют те же агенты, что и в самой распространенной «иерархической» (крупное — малые предприятия), но связь

между ними по линии «заказчик — подрядчик» обратная. То есть, в центре такой сети располагается не значительное и авторитетное в своей сфере предприятие, а мало кому известная частная фирма небольших размеров, рекрутирующая для выполнения своих производственных задач крупных производственных партнеров.

Схема родилась не из головы, а из реального опыта. Фактором, повлиявшим на появление таких перевернутых экономических отношений, явилось становление отечественного инновационного бизнеса. Малые наукоемкие предприятия, отпочковавшиеся от бюджетной науки, вынуждены доводить свои разработки до стадии изделий, следовательно, — обращаться к крупным заводам, преимущественно военно-промышленного комплекса. Очевидно, что перевернутые по «весу» отношения (малое предприятие является заказчиком у большого) специфичны именно для переходной экономики, а также — для инновационного сектора, обреченного на альянс именно с крупными технологически развитыми предприятиями ввиду своих завышенных технических требований.

Зафиксировав реальное явление, зададимся вопросом: насколько оно долговечно? Пробивает ли такой тип кооперационных отношений себе дорогу в условиях новой экономики, либо является временным феноменом, следствием резкой трансформации экономического строя? Для ответа на это вопрос рассмотрим динамику взаимодействия партнеров в условиях «перевернутой» иерархической модели.

Поведение крупных предприятий и их подразделений с мелкими фирмами-заказчиками легко интерпретируется через ключевое понятие социальной (в том числе экономической) власти. Крупные организации и их представители, будучи технологическими монополистами, нередко действуют в личных интересах, аккумулируя власть и прибыль, причем намного чаще, чем в интересах деловой «эффективности» или заботе о социаль-