### Современные технологии обеспечения информационной безопасности

### Введение

Со стремительным развитием Интернет-технологий многие ведущие зарубежные фирмы, специализирующиеся в сфере информационных технологий, ежегодно вкладывают огромные средства в создание соответствующего инструментария интеллектуальной обработки текстовой, речевой и графической информации.

В первую очередь, это связано с тем, что на применении названных интеллектуальных технологий обработки данных базируются перспективные концепции управления силами и средствами в сложной обстановке. Сегодня на основе их активного использования предполагается поддерживать политические, экономические и иные решения. На их базе строятся и сложные биометрические системы идентификации и верификации как в интересах государственных и правоохранительных структур, так и для решения задач обеспечения безопасности коммерческих организаций.

Конечно, интеллектуализация обработки данных в связи с бурным развитием Интернет-технологий начинает приобретать все большее значение для эффективного решения двух основополагающих проблем.

С одной стороны, это получение в реальном масштабе времени многоаспектной и объективной информации из Интернет, других доступных информационных и телекоммуникационных систем о состоянии, направлении развития и уровне угроз тех или иных процессов в мировом масштабе, обществе и его отдельных этно- экономических образованиях. Очевидно, что синтез знаний, отраженных в тех или иных разрозненных и, на первый взгляд, не связанных единой логикой данных, осуществленный на основе систем их интеллектуальной обработки, дает абсолютно новое интегративное качество, позволяющее предугадать, а значит - и предупредить негативное развитие тех или иных процессов и явлений. Таким образом, речь идет о создании на базе названных технологий, интеллектуальной среды моделирования безопасного развития систем и процессов.

С другой стороны, применение интеллектуальных технологий обработки данных дает возможность на порядок повысить безопасность функционирования различных компьютеризированных систем, в том числе связанных с принятием стратегических решений, отвечающих за безопасное развитие технологических процессов, используемых в системах управления войсками и оружием. Понятно, что на смену наиболее распространенным PIN и подобным технологиям, весьма уязвимым с точки зрения безопасности компьютеризированных систем, должны придти и уже приходят более продвинутые и надежные технологические решения, связанные, в частности, с биометрикой. Не могу не сослаться в этой связи на утвержденную 9 сентября 2000 года российским Президентом «Доктрину информационной безопасности Российской Федерации», где прямо говорится о необходимости создания новых средств и систем предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий.

Из сказанного хотелось бы сделать вывод: в условиях быстроменяющейся международной и внутриполитической обстановки в России, характеризующейся выраженным дефицитом времени на принятие стратегических решений, связанных с глубоким анализом и прогнозированием развития ситуации в различных сферах жизнедеятельности, ориентация на интеллектуальные автоматизированные системы подготовки решений и защиты информации применительно к нашей стране выступает в качестве первоочередной задачи.

### Перспективные технологии защиты информации

Выступивший на конференции заместитель начальника Главного управления ФАПСИ д.ф-м. Н. А Кузьмин в своем докладе о перспективных технологиях обеспечения информационной безопасности подчеркнул, что в современном обществе уровень решения проблем защиты информации, наряду с прогрессом компьютерных технологий, стал фактором, определяющим скорость и эффективность внедрения информационных технологий во все сферы жизни. Более того, на его взгляд, от качества применяемых технологий защиты информации зависит сейчас не только сохранность в секрете конфиденциальных сведений, но и вообще существование конкретных информационных и телекоммуникационных сервисов, услуг и приложений.

В настоящее время в России и за рубежом, как отметил докладчик, активно развиваются и внедряются криптографические компьютерные технологии, направленные на обеспечение работоспособности таких комплексных и масштабных сетевых приложений, как электронный банк (e-banking), электрон ная торговля (e-commerce) и электронный бизнес (e-business). По вполне понятным причинам среди этих технологий определяющую роль играют криптографические протоколы аутентификации, распределения ключей и системы электронной цифровой подписи (ЭЦП).

А Кузьмин считает, что важной проблемой здесь является обеспечение эффективного отображения арсенала существующих и новых перспективных криптографических решений (алгоритмов, протоколов, ключевых систем) на все расширяющееся множество прикладных программных продуктов, сетевых операционных систем и аппаратных платформ, на которых базируются упомянутые выше информационные системы и ресурсы. В этой связи, по словам докладчика, на повестке дня стоят и поэтапно решаются (в том числе под руководством и с участием ФАПСИ) задачи разработки, совершенствования и внедрения следующих важнейших технологий защиты информации:

* новых стандартов ЭЦП;
* масштабируемой системы электронных цифровых сертификатов с использованием центров доверия;
* криптографически защищенных корпоративных (виртуальных) компьютерных сетей и средств межсетевого экранирования;
* средств антивирусной защиты и средств защиты от несанкционированного доступа (НСД) к информации для неоднородных распределенных информационных систем;
* мониторинга и аудита безопасности сетевых информационных ресурсов;
* защищенных программно-аппаратных средств для IP-телефонии;
* средств защиты сетей мобильной связи и персональных коммуникаций;
* средств биометрической идентификации, а также персональных СКЗИ и средств аутентификации на базе интеллектуальных карт и других малогабаритных технических средств обработки информации.

На взгляд докладчика, развитие указанных перспективных технологий защиты информации требует, с одной стороны, применения новых математических и криптографических решений (например, криптоалгоритмов на основе эллиптических кривых, методов квантовой криптографии, фрактальных алгоритмов сжатия данных), а, с другой стороны, существенно зависит от прогресса в уровне развития отечественных микропроцессорных, алгоритмических, программистских и других смежных технических решений.

Перспективные технологии защиты информации должны синтезировать только высокотехнологические разработки интеллектуальных систем анализа информации, интегрирующих передовые достижения лингвистического анализа, речевых технологий, визуализации данных, программно-технических решений. Именно в этих сферах деятельности сосредоточены лучшие силы программистов и специалистов по компьютерным технологиям и информационной безопасности. Россия здесь не является исключением.

Состояние российских исследований в области интеллектуальных систем анализа и защиты информации, говоря в целом, нельзя охарактеризовать даже как удовлетворительное. Однако, парадоксально, но факт - несмотря на катастрофическое состояние науки и сферы производства, нехватку средств на разработку и исследования, приоритет на многие передовые технологические решения в этой сфере принадлежит российским специалистам. Объяснение этого феномена весьма просто. Если говорить коротко, оно связано с двумя позитивными явлениями:

* – в наследство новой России, с ее разрушенной экономикой и развалившейся научно-производственной базой досталась довольно широкая прослойка высококлассных математиков и программистов, по российской же традиции в условиях хронического безденежья продолживших свои изыскания.
* – в предчувствии резкого изменения конъюнктуры рынка в сторону высокотехнологичных интеллектуальных средств и систем анализа и защиты информации многие фирмы, в основном - коммерческие осуществляли финансовые вливания в их исследования и разработку. Здесь нужно заметить, что предчувствие основывалось на вполне объективной информации, исходившей от коллег - российских специалистов, эмигрировавших за рубеж и работающих по контрактам с зарубежными фирмами.

### Перспективы применения биометрических технологий идентификации

О перспективности биометрических технологий идентификации, относящихся к интеллектуальным технологиям, говорит и недавний шаг Microsoft, лицензировавшей биометрическую технологию и программную систему биометрической идентификации пользователей ее разработок. В биотехнологических разработках уже проявили себя компании Compaq, Identix, Veridicom, Key Tronic, Miros, Visionics и др.

Ведущий специалист из Института автоматизации проектирования РАН д.ф.-м.н А.С.Глазунов отметил, что следующую закономерность в затратах на построение биометрических систем идентификации личности. Если выстроить эти системы в ряд с точки зрения затрат, то получится примерно следующая последовательность: голос - сетчатка - радужная оболочка - палец - подпись - рука - лицо. Он также отметил, что использование биометрических систем в полной мере, несмотря на возрастающий спрос, пока достаточно ограничено. Главные причины лежит в относительной сложности интеграции подобных систем с персональным компьютером, подчас неудобстве использования, сравнительно низкой надежности и эффективности.

Существуют и проблемы законодательного характера. Об их остроте говорит хотя бы тот факт, что, например, в США уже давно дискутируется вопрос о применении биометрических технологий, в том числе понижения вероятности введения запретительных законов, резко ограничивающих области их использования.

Следует также отметить, что эффективность биометрических систем еще недостаточно велика по ряду причин. Главный вопрос здесь - как будут вести себя биометрические системы идентификации при размерах баз данных, когда число пользователей будет превышать миллион и более.

Говоря о биометрических технологиях обеспечения информационной безопасности, нельзя не упомянуть о проблеме восстановления и шумоочистке программными методами аудиосигналов, в том числе - речи. В последние годы российскими специалистами здесь достигнуты определенные успехи. Об этом говорил в своем выступлении к.т.н. Дворянкин С.В., заместитель начальника факультета информационных технологий Московского института МВД России, много лет занимающийся этими вопросами в связи с решением задач обеспечения информационной безопасности. В частности, он отметил, что сегодня разработано большое количестворазличных устройств и программ, способных повышать качество звучания или разборчивость человеческой речи. Среди них наиболее развиты системы обработки, использующие фильтрацию и компенсацию помех, спектральное вычитание, коррекцию и сглаживание амплитудно-частотной характеристики звукового тракта адаптивного подавления помех, методы линейного предсказания, "псевдостерео" и другие. Такого рода системы предназначены для реализации одного или нескольких методов обработки, настроенных под конкретный вид помехи и/или канал связи. Это весьма неудобно, поскольку все возможности имеющегося сегодня арсенала методов восстановления разборчивости и качества речи, искаженной различного рода помехами и шумами, можно ощутить, используя только весь парк традиционных и специализированных звуковых редакторов.

Более того, как отметил С. Дворянкин, большинство представленных сегодня на рынке программных продуктов либо требуют высокой профессиональной подготовленности пользователя, либо имеют отставание в интерфейсе от требований современных операционных систем, либо обладают ограничениями на выбор типа компьютера, работу только в одной операционной системе и только с одним видом звуковых карт, либо страдают из-за отсутствия регулярных сопровождения, поддержки и обновления, либо просто очень дороги. В то же время, очевидно, что наибольшим успехом у пользователя, ограниченного во времени и владеющего элементарными познаниями в области цифровой обработки сигналов и изображений, будут пользоваться звуковые редакторы с мощной математической и физической подоплекой и, в то же время, с хорошим дружественным интерфейсом, не требующим специальных математических познаний и не задающим вопросов типа "Какой фильтр выбрать?", "Каким окном взвешивания воспользоваться?" и т.п.

### Технологии защиты информации на основе идентификации голоса

Участников конференции весьма заинтересовали технологии защиты информации на основе идентификации голоса, представленные специалистами Центрального научно-исследовательского института машиностроения (ЦНИИМАШ) к.ф.-м.н Д. Коноваловым и А.Бояровым. Содокладчики представили комбинированную систему, состоящую из блоков идентификации и верификации голоса.

При решении задачи идентификации находится ближайший голос (или несколько голосов) из фонотеки, затем в результате решения задачи верификации подтверждается или опровергается принадлежность фонограммы конкретному лицу. Система практически используется при обеспечении безопасности некоторых особо важных объектов.

Д.т.н. Л. Чудновским (профессор МГИМО) представлены новые технологии передачи скрытой информации в речевом сигнале. Для этого им использованы такие временные участки речевого сигнала, которые неважны для восприятия человека.

Среди особенностей психоакустики он выбрал "эффект маскировки". Суть его состоит в следующем. Более интенсивные речевые отрезки делают неслышимыми сигналы, появившиеся до них («маскировка вперед») и после них («маскировка назад»). Временной диапазон маскировки вперед простирается до 20 мс, а назад – до 150 мс. Кроме того, существует и частотная маскировка, когда в момент появления более интенсивного низкочастотного сигнала становится неслышным более высокочастотный сигнал меньшей амплитуды.

Скрытую информацию можно внедрять также, используя ограничения, связанные с разрешением аудиосистемы человека. Например, нечувствительность слуховой системы к провалам спектра в шумовом сигнале. Таким образом, можно на звуках речевого сообщения, порожденных турбулентным источником (звуки [х], [ш], [с]) передавать дополнительную информацию.

За счет такого рода особенностей человеческого слуха скорость передачи скрытой информации может составить до 100 бит в секунду. Любопытно, что и скорость передачи, так сказать, "легального" компонента речевого сигнала составляет 50-100 бит в секунду.

### Оптимальные модели управления компьютьерными системами в условиях противодействия вредоносным программам

Как показала конференция, высокими технологиями в сфере обеспечения информационной безопасности обладают не только столичные специалисты, но и представители других регионов. Оригинальную, научно обоснованную разработку, направленную на противодействие компьютерной преступности при обработке информации в автоматизированных системах управления (АСУ) различного назначения, продемонстрировал д.т.н. С.Скрыль из Воронежского института МВД России.

Если системы защиты информации (СЗИ) традиционно разрабатываются как системы, в которых функции защиты сосредотачиваются в рамках одной из подсистем АСУ, то автором предложено эти функции рассредоточить по всему информационному процессу. Это позволяет существенно сократить время, затрачиваемое на идентификацию несанкционированного манипулирования информацией, что особо актуально при противодействии преступлениям с использованием так называемых вредоносных программ – программ вирусного типа, ориентированных на преодоление систем защиты информации с последующим несанкционированным манипулированием данными АСУ.

Таким образом, подход к решению данной проблемы, основанный на применении средств противодействия вредоносным программам, встраиваемых в программы обработки информации в компьютерных системах, позволяет обеспечить соизмеримость периода применения средств противодействия с временными параметрами вредоносных программ и повысить возможности обнаружения таких программ. При этом методики временного резервирования в интересах организации противодействия вредоносным программам содержат элементы новизны как по сути, так и по области применения.

Представляют большой интерес разработанные автором математические модели процессов функционирования компьютерных систем в условиях противодействия вредоносным программам, позволяющие оценивать различные параметры средств противодействия и способы их применения. Разработанный математический аппарат позволяет решать задачи временного резервирования процессов функционирования АСУ применительно к различного рода угрозам их информационным процессам; а c практической точки зрения, - проектировать и разрабатывать программное обеспечение АСУ, устойчивое к негативным воздействиям, возникающим вследствие проникновения в АСУ компьютерных вирусов.

Комплексный подход к анализу организации противодействия вредоносным программам, позволяет выработать ряд важных практических рекомендаций и экспериментально доказать целесообразность его применения. Автором разработана технология проектирования программного обеспечения компьютерных систем, реализующего функции обнаружения воздействия негативных факторов, связанных с несанкционированными действиями в отношении информации, в процессе выполнения функций по ее обработке. Применение такой технологии наиболее эффективно при организации защиты информации от воздействия программных средств хищения и искажения данных вирусного типа, характеризующихся крайне незначительным временем своего проявления. Это позволяет достигать повышения эффективности противодействия таким программам на 25-30 %.

Значимость и актуальность проблемы борьбы с компьютерными вирусами были отмечены специалистами ФАПСИ И. Добрицей, А. Ждановым и С. Захаровым в их докладе, посвященном требованиям к антивирусным средствам.

Авторы подчеркнули, в связи с тем, что в настоящее время на рынке представлен широкий спектр антивирусного программного обеспечения (ПО) отечественного и зарубежного производства как хорошего, так и сомнительного качества, как никогда актуальна проблема выбора качественного инструментария для построения эффективной и надежной антивирусной защиты автоматизированных информационных систем (АИС).

Для решения данной проблемы ФАПСИ совместно с рядом ведущих отечественных разработчиков антивирусных средств (АВС) разработаны требования к антивирусным средствам.

Требования устанавливают классификацию АВС по их функциональным возможностям и способам использования в АИС на основе перечня показателей и совокупности предъявляемых к ним требованиям по обеспечению антивирусной защиты. Устанавливается 7 классов АВС. Каждый класс описывается перечнем показателей (обнаружение, лечение, блокирование, восстановление, регистрация, обеспечение целостности, обновление базы данных, компьютерных вирусов, защита АВС от доступа паролем, средства управления, гарантии проектирования, документация) и совокупностью требований по обеспечению антивирусной защиты, предъявляемых к каждому показателю. В каждом классе предусмотрены два подкласса в зависимости от степени секретности обрабатываемой информации.

Авторы считают, что Требования к антивирусным средствам учитывают все многообразие АВС и перспективы их развития, позволяют выбрать качественный инструментарий для построения эффективной антивирусной защиты.

### Проблема интеллектуального анализа данных и обеспечения информационной безопасности

На конференции шла речь и об одной из перспективных российских разработок в сфере интеллектуального анализа данных и обеспечения информационной безопасности. Она осуществляется коллективом специалистов отделения «Методология и моделирование безопасного развития систем и процессов» Российской Академии естественных наук, представляющих высокотехнологичные сферы отечественной науки и объединившихся для создания интеллектуальных систем подготовки решений и защиты информации.

К настоящему времени ими найдены эффективные решения в сфере интеллектуальной обработки данных, не имеющие аналогов в мировой практике и превосходящие по своему уровню достижения зарубежных специалистов.

Так, этой группой ученых создан специальный метаязык «ДИАЛ», позволяющий структурировать сложное семантическое пространство естественных языков и оптимизировать аналитическую деятельность в самых разных сферах подготовки решений.

Создание метаязыка дало возможность принципиально преодолеть две основные проблемы, препятствовавшие реализации интеллектуальных систем нового поколения. А именно, проблему многоязычия и проблему поиска актуальной информации и эффективной навигации в Интернет.

Использование метаязыка позволило решить ряд прикладных задач, знаменующих качественный прорыв в области машинного перевода. В настоящее время осуществляется профессиональный автоматизированный перевод между восемнадцатью распространенными языками мира, включая русский. Наращивание дополнительных языков не представляет какой-либо принципиальной сложности.

Другой важнейшей прикладной задачей, решенной учеными, является составление в реальном масштабе времени рефератов текстовой информации, в том числе - циркулирующей в Интернет.

Очевидно, что эти возможности, реализованные в применяемых на практике интеллектуальных системах, позволят существенно поднять производительность и качество труда аналитической деятельности и на порядок расширить ее информационное поле, масштабность и глубину анализа. Значительно повышается и прогнозирующая функция в работе аналитиков, что позволяет довести принятие упреждающих решений до необходимого системного уровня. Понятно, что результаты решения обеих задач напрямую связаны с вопросами обеспечения информационной безопасности.

Внедрение интеллектуальной автоматизированной компоненты в аналитическую деятельность различных структур позволяет кардинально улучшить подготовку управленческих решений как стратегического, так и тактического

уровня. Особо следует подчеркнуть, что при этом не так важна собственно вычислительная мощность аналитической системы по сравнению с ее интеллектуальной составляющей.

Сущность этих технологий заключается в интеллектуализации управления процессами информационного обеспечения человека. Здесь и автоматизированный поиск информационных взаимосвязей любых объектов - событий, людей, телефонных переговоров, адресов и т.д. из всех видов баз данных, существующих в мире. И визуализация сложно структурированной информации в графическом и табличном виде. И статистический и географический анализ событий. И нахождение скрытых, латентных объектов.

Выступающие на конференции разделили вывод автора настоящей статьи о том, что пришло время практического создания интеллектуального телепортала, основное предназначение которого – интеллектуальная системная обработка информации всех видов. Однако до сих пор программные компоненты, направленные на обработку речевой и графической (фотографии, рисунки и т.п.) и в определенной мере - текстовой (в смысле лингво-анализатора) информации не синтезированы в единую систему. Между тем, как свидетельствуют выступления ведущих специалистов на данной секции, предпосылки для успешного решения задачи информационного синтеза имеются. Важность решения этой задачи, в частности, для кардинального изменения системы обеспечения информационной безопасности понятна.

Таким образом, разработкам российских специалистов, относящимся к созданию интеллектуального телепортала, необходима государственная поддержка. В противном случае названные разработки могут оказаться достоянием структур, заинтересованных в торможении процесса качественного преобразования аналитической деятельности в России. Более того, не исключена возможность перехода их тем или иным путем в руки зарубежных фирм или даже - криминальных групп. В конечном итоге, обладание интеллектуальными технологиями обработки информации, по большому счету напрямую затрагивает и вопрос обеспечения национальной безопасности.

### Нетрадиционные подходы противодействия организованной преступности на основе информационных технологий

Об опасности, когда криминальный мир активно овладевает современными информационными технологиями, говорил в своем докладе д.т.н. А.Овчинский, начальник факультета Московского института МВД России.

В докладе говорилось об осуществлении активных информационных воздействий как на лидеров и членов преступных формирований, так и на связанных с ними лиц. Эффективность таких воздействий может быть обеспечена применением современных радио и телекоммуникационных средств, Интернета, средств массовой информации.

Докладчик подчеркнул, что концепции информационных войн, перенесенные на практику борьбы с преступностью, указывают на то, что любым мероприятиям, направленным на противодействие преступным формированиям, на подрыв их финансовых основ, экономической базы, на ликвидацию коррупции в структурах власти, должно предшествовать информационно-техническое обеспечение.

### Системы управления информационной безопасностью коммерческих организаций

Интерес слушателей, среди которых было много предпринимателей, вызвал доклад д.т.н., профессора, академика РАЕН О.Викулова, представлявшего Центральный научно-исследовательский институт радиоэлектронных систем, в котором шла речь о системе управления информационной безопасностью коммерческих организаций.

Он акцентировал внимание на том, что как свидетельствует реальность, злоумышленные действия над информацией применительно к коммерческим организациям не только не прекращаются, а имеют достаточно устойчивую тенденцию к росту. Опыт показывает, что для успешного противодействия этой тенденции необходима стройная и управляемая система обеспечения безопасности информации.

При этом докладчик заметил следующее:

* - объектом защиты становится не просто информация как некие сведения, а информационный ресурс, т.е. информация на материальных носителях (документы, базы данных, патенты, техническая документация и т.д.), право на доступ к которой юридически закреплено за ее собственником и им же регулируется;
* - информационная безопасность пользователей в отличие от физической обеспечивает защищенность их прав на доступ к ИР для удовлетворения своих информационных потребностей;
* - с точки зрения экономической целесообразности защищать следует лишь ту информацию, разглашение (утечка, потеря и т.д.) которой неизбежно приведет к материальному и моральному ущербу.

Викулов обосновал принципы обеспечения безопасности информационных систем:

* Законность мероприятий по выявлению и предотвращению правонарушений в информационной сфере;
* Непрерывность реализации и совершенствования средств и методов контроля и защиты информационной системы;
* Экономическая целесообразность, т.е. сопоставимость возможного ущерба и затрат на обеспечение безопасности информации;

Комплексность использования всего арсенала имеющихся средств защиты во всех подразделениях фирмы и на всех этапах информационного процесса.

Он также отметил, что в зависимости от масштаба и вида деятельности коммерческой организации структура ее СИБ может быть разнообразной, исходя из экономической целесообразности. Однако обязательными элементами, присутствующими в ее структуре и соответствующими основным направлениям защиты, должны быть следующие:

Правовая защита – юридическая служба (юрист, патентовед, рацорг, оценщик интеллектуальной собственности т.п.), взаимодействующая с бухгалтерией и плановым отделом;

Организационная защита – службы охраны (комендант, контролеры, пожарные и т.п.) и режима (государственной, служебной тайны, конфиденциальной информации и т.п.), взаимодействующие с отделом кадров;

Инженерно-техническая защита – инженерно-техническая служба (операторы ЭВМ, связисты, криптографы, техники и т.п.), взаимодействующие с функциональными подразделениями фирмы.

По мнению профессора, объединяющим и координирующим началом всей системы информационной безопасности (СИБ) является ее начальник в ранге заместителя руководителя фирмы по безопасности, опирающийся в своих действиях на решения Совета безопасности, объединяющего начальников соответствующих служб и возглавляемого ответственным руководителем фирмы.

Он также считает, что функционально СИБ строится в виде перекрывающихся “концентрических” контуров защиты по отношению к внешним угрозам, в центре которых располагается объект защиты. При этом “внешним” контуром (большего “радиуса”) является контур правовой защиты, обеспечивающий законность и правомерность как самого объекта, так и мер по его защите. Далее следует контур организационной защиты, обеспечивающий порядок доступа к объекту, который непосредственно защищается “внутренним” контуром инженерно-технической защиты путем контроля и предотвращения утечки, НСД, модификации и потери информации.

Такое построение СИБ позволяет существенно локализовать техническую защиту и сократить расходы на нее вследствие правовой “селекции” объектов защиты и организации ограниченного доступа к ним.

Судя по количеству заданных профессору вопросов, в современных коммерческих структурах проблеме информационной безопасности уделяется неослабное внимание, и что она является крайне актуальной в условиях обострения конкурентной борьбы, проявляющейся в виде многих фактов промышленного шпионажа.

**В.А.Минаев,**