Римляне построили дороги – и появились разбойники. Англичане создали флот – и появились пираты. Американцы придумали компьютеры – и на них паразитируют хакеры. Дороги, флот и ЭВМ строились без учета защищенности. Интересно, что будет, когда мы создадим защищенный семантический компьютер?

В.А.Конявский

Для современного общества, основное свойство которого – развитие цифровых технологий во всех сферах, крайне важной задачей является поиск новых путей информационных технологий и инструментов решения острых проблем информационного общества. В этой ситуации предназначение истинного ученого – прислушаться к тем, кто стоял у истоков, осознать актуальные особенности развития общества как логическое следствие из созданных ранее фундаментальных основ науки и практики, сформировать новую научную парадигму.

Фундаментальные исследования Валерия Аркадьевича Конявского, доктора технических наук, академика РАЕН, заведующего кафедрой «Защита информации» МФТИ, имеют огромное значение в области технической защиты информации на современном этапе развития наук об информации. Сегодня мы публикуем беседу с этим выдающимся ученым на затронутые актуальные темы.

Валерий Аркадьевич, у Вас невероятно большой опыт в сфере безопасности и защиты информации. На Ваш взгляд, какая проблема в настоящее время наиболее актуальна в данной научной сфере?

Принципиальное отличие нашего времени – появление систем цифровой экономики. Все исследования в области технической защиты информации до последнего времени проводились с учетом того, что мы работаем с корпоративными системами, границы которых точно известны.

В этих границах всегда можно обеспечить достаточный уровень защищенности, базирующийся на доверенности СВТ, включенных в состав системы.

В открытых же системах ставить вопрос об обеспечении доверенности всех средств вычислительной техники просто невозможно. Так, мобильные средства доступа пользователей ни при каких условиях нельзя сделать доверенными.

В рамках корпоративных систем нет проблемы обеспечить всех участников сертифицированными идентификаторами и выполнять операции по аутентификации в доверенной среде. Требуются только деньги – самый недорогой из ресурсов. В открытой же системе этого добиться невозможно. Невозможно повлиять на китайскую промышленность, ориентирующуюся на рост объемов при снижении цен. Обращаясь за госуслугами, телемедицинскими консультациями, услугами банков, услугами в секторе B2C, граждане всегда будут пользоваться смартфонами, о доверенности которых говорить не приходится. Такой доступ всегда будет самой «легкой добычей» для всех видов атак с использованием вредоносного ПО.

Таким образом, можно сказать, что недоверенные СВТ – важнейшая, системная характеристика среды идентификации в цифровой экономике.

Значит ли это, что Вы считаете невозможным применение в недоверенной среде методов, разработанных именно для доверенной среды?

Здесь необходимо остановиться на проблеме идентификации. В корпоративной системе все ясно: доверенный терминал, криптография, многофакторная идентификация. Было бы неплохо все население мира обеспечить доверенными смартфонами и токенами, но это особый вид фантазий, далекий от реальности. В качестве инструмента идентификации мы можем использовать цифровую биометрию, но проблема заключается в том, что ставить

криптографию на недоверенный смартфон бессмысленно.

Успешный опыт применения биометрии связан только с криминалистической идентификацией – предполагается, что в базах данных никто отпечатки не подменит, гражданин не наденет при регистрации перчатку и не передаст ее потом злоумышленнику, а средства идентификации, используемые полицией – доверенные.

Криминалистика, как правило, имеет дело с людьми, не ориентированными на сотрудничество. Ее обычный объект – это труп, подозреваемый или преступник. Цель анализа – доказать факт совершившегося доступа объекта к орудию и/или месту преступления, установление личности потерпевшего и так далее. И, конечно, объект обычно совсем не заинтересован в правильной идентификации.

Активное противодействие здесь, как правило, либо отсутствует, либо направлено на нарушение идентификации – доказать, что на месте преступления не был, в противоправных действиях не участвовал, закона не нарушал.

Используемые технические средства при этом – доверенные. Они специально разрабатываются, защищаются сертифицированными средствами, проходят регламентные процедуры контроля и так далее.

В цифровой экономике объект идентификации - вполне живой и добропорядочный участник экономической деятельности. Пример его потребности – получить доступ к некоторым ресурсам. Он готов к сотрудничеству, готов выполнить некоторые действия, чтобы после успешной идентификации получить нужную ему услугу, поэтому заинтересован в правильной идентификации.

Таким образом, процессы идентификации в криминалистике и цифровой экономике полностью различны.

Не совпадают:

- объекты идентификации;
- их одушевленность/неодушевленность;
- заинтересованность объекта идентификации в ошибке;
- желательный для объекта идентификации результат;
- характер участия объекта в процессе идентификации.

При этом противоположными являются:

- контролируемость инструмента субъектом;
- доверенность среды идентификации;
- значимость того, жив ли объект идентификации;
- значимость согласия объекта идентификации с результатом идентификации;
- заинтересованность объекта идентификации в подтверждении гипотезы субъекта.

При таком глубоком различии процессов представляется странным использование одинаковых инструментов, и, отвечая на Ваш вопрос, можно утверждать, что применение в недоверенной среде методов, разработанных для доверенной среды, не имеет смысла. Отметим, что инструменты и методы в данном случае предназначены для обработки данных, а не их порождения. И для каждой цели нужно выбирать те данные, которые содержат необходимую информацию.

Что Вы думаете о применяемых для идентификации методах анатомии и физиологии?

В силу простоты и статичности применяемые модальности (папиллярный узор, радужная оболочка и сетчатка глаза, сосудистое русло и другие) легко воспроизводятся и моделируются, что не только не снижает риски ошибочной идентификации, но и позволяет непосредственно влиять на ее результаты. Традиционные (инвариантные к внешним факторам) биометрические модальности не обеспечивают и не могут обеспечить достаточный уровень доверенности идентификации на недоверенном устройстве, так как исследования по применению биометрических механизмов явно или неявно основываются на предположении о доверенности технических средств обработки.

В нашем случае (цифровая экономика) это предположение явно неверно, и именно поэтому необходимо изменить подход к биометрическим характеристикам как к инвариантам.

Для устранения уязвимостей, связанных с простотой подмены измерений на недоверенных устройствах, необходимо от статических показателей перейти к динамическим типа «стимул-реакция» со сложной динамикой связи. Динамическим звеном, чрезвычайно

сложным на сегодняшний день для моделирования, являются нервная и вегетативная системы человека и, связанные с этим, особенности физиологии движений. В частности, индивидуальными оказываются непроизвольные реакции на внешние стимулы (например, аудио и видео раздражители).

Реакция на стимулы может быть зафиксирована датчиками клиентского устройства, обработана с помощью методов искусственного интеллекта, например, искусственных нейронных сетей, что позволит определить источник потоков данных и повысить достоверность идентификации.

Возможности смартфона среднего ценового сегмента в части определения биометрических характеристик практически ограничены камерой. Какие динамические характеристики может определять такой смарфон?

Из динамических биометрических характеристик человека надежно можно зафиксировать, по крайней мере, характеристики пульсовой волны, динамику изменения диаметра зрачка, динамику слежения взглядом за стимулом на экране. Для этого достаточно на смартфоне иметь камеру и вспышку (фонарик), а также сенсорный экран.

Перспективным является изучение движения глаз. Достаточно отметить, что движениями глаз управляют 7 мышц (!), и мышцы, ответственные за саккадические движения, являются самыми быстрыми. Многообещающим представляется изучение рефлекторной составляющей саккад, а также (а может, и в первую очередь) процессы фиксации и регрессии при чтении. Основными динамическими рефлекторными модальностями, которые предлагают актору непривычную для мозга работу, могут быть: рассогласование взгляда и стимула при слежении за движущейся точкой, поиск слова в таблице, заполненной случайными символами алфавита, движение глаз при чтении отрывка текста после слияния слов.

Реакции человека на внешние стимулы существенно зависят от когнитивных и кинезиологических особенностей человека, носят динамический характер и отражаются в измерениях в достаточной для анализа степени.

Принципиальными особенностями предложенной системы стимул-реакция является наличие нервной системы человека как связующего звена между стимулом и реакцией и возможность давать случайные, не повторяющиеся стимулы. При этом обработка пары стимул-реакция может производиться на удалённом доверенном устройстве. Как следствие, данная система имеет следующие преимущества:

- Недоверенность клиентского терминала не влияет на результаты, так как генерация стимула и анализ реакции выполняется на отчужденных доверенных ресурсах, а искажение реакции не даст возможности злоумышленнику получить нужный для него результат;

- Перехватывать стимул нет смысла, так как, зная стимул, невозможно сгенерировать реакцию в силу отсутствия модели человека;

- Извлечь параметры нейронной сети путем ее тестирования невозможно;

- Акты идентификации уточняют параметры нейронной сети, и поэтому даже тотальное наблюдение не позволит в полной мере воспроизвести сеть.

Известно, что на любую проблему в конкретной области для ее успешного решения необходимо воздействовать комплексно и создавать все необходимые для этого условия. На Ваш взгляд, что нужно сделать, чтобы ускорить прогресс в области информационных технологий и в частности - в сфере информационной безопасности?

Здесь нужно начать, так сказать, от истоков, и для этого вспомним о таких тесно взаимосвязанных категориях, как смысл и безопасность.

Целое – это единство формы и содержания. Во всяком случае, если мы говорим о реальности.

Разрыв формы и содержания – самый характерный признак мирового развития computer science, который заметен уже начиная с аналитической машины Чарльза Беббиджа, универсального вычислителя Тьюринга, принципов и архитектуры фон-Неймана и других, и заканчивая решениями нынешнего времени.

Все известные универсальные вычислители сегодня являются именно **вычислителями**.

Они работают с формой – числами. Процесс выполнения операций над числами никак не связан с содержанием, с семантикой. Именно с отрывом формы от содержания, на мой взгляд (здесь и всюду далее наиболее жесткие аттестации – это мое оценочное мнение), связаны все основные проблемы в развитии информационных технологий, базовые принципы которых уже нельзя считать ничем иным, как фатальным заблуждением. Мысль не продвинулась дальше больших калькуляторов с хорошими экранами.

Действительно, любая ЭВМ легко вычислит 5+6, и даст на первый взгляд верный ответ – 11. Но чего – 11? Если 5 – это яиц, а 6 – помидоров, то результат – это одна яичница из 5-и яиц и 6-и помидоров, а никак не 11. Да и «одна яичница» – верный ответ лишь в том случае, если 5 яиц и 6 помидоров положили на горячую сковороду. А если в холодильник – то 5+6 на утро будет снова 5+6.

Числа – это только форма. Содержание утеряно, за числами не стоит семантика. Вычисления приходится интерпретировать, а негодяям повлиять на интерпретацию очень несложно, так как интерпретация осуществляется, как правило, за пределами контролируемой зоны, на произвольных программных и технических средствах. Именно ошибочные интерпретации и приводят зачастую к удачным хакерским атакам, подменам смысла и прочим неприятностям.

Все время своего существования вычислительная техника развивалась в сторону ускорения вычислений, уменьшения размеров и повышения универсальности. Мощность современного смартфона выше совокупной мощности всех ЭВМ в мире в 60-х годах прошлого столетия. А ведь тогда уже были мэйнфреймы IBM. Универсальность выросла настолько, что бухгалтер и дизайнер используют одинаковые компьютеры с одинаковыми офисными пакетами, а программистами в быту стали называть людей, способных освоить хотя бы одну сложную программу – например, фотошоп.

Любой компьютер – это реализация (более или менее близкая) идеи «машины Тьюринга». Понятия «машина Тьюринга» и «алгоритм», вычислимость – неразрывно связаны, определяются одно через другое. Само существование абстрактного «исполнителя», такого, как машина Тьюринга, – вселяет уверенность во всемогуществе человека. Действительно, любая (точнее, рекурсивная, что и есть практически любая) задача может быть решена, если достаточно ресурсов (памяти и времени). Возможно, завораживающая простота формулировок и спровоцировала разработку универсальных вычислительных машин (УМ) которые частично (с конечной памятью) моделируют машину Тьюринга, давая нам псевдо «неограниченные» возможности и толкая на экстенсивный путь развития. Не хватает памяти – что за проблема, – добавим. Не хватает времени – увеличим тактовую частоту, количество ядер, виртуализируем ресурсы, наконец.

Эта позиция многие годы «паровозом» тащила за собой развитие информационных технологий. Емкость обычных локальных дисков, например, за два десятилетия выросла от десятков килобайт до сотен гигабайт и уже измеряется терабайтами, а памяти так и не хватает. Тактовые частоты от килогерц достигли гигагерц, а производительности не хватает. Зато индустрия ИТ стала едва ли не определяющей современный уровень экономического развития. Гигантские суммы инвестиций – плата за технический прогресс и универсальность решений.

Универсальность (в смысле «вычислимости», без учета семантики) опасна и снижением защищенности. Действительно, если УМ выполняет любые программы, то, очевидно, она выполнит и вредоносную программу. Несмотря (!) на любой набор антивирусных программ. Действуя в рамках пусть универсальной, но одной формальной модели, мы неизбежно натолкнемся на ее неполноту – в полном соответствии с теоремой Геделя о неполноте.

В результате работы с функциями был сформулирован тезис Черча-Тьюринга, утверждавший, что любая функция, которая может быть вычислена физическим устройством, может быть вычислена машиной Тьюринга. Вычислена. И только. А не осмыслена. А надо бы осмыслить.

Говоря о вычислимости, классики «забыли» о семантике. Они думали именно о вычислимости, и здесь в их рассуждениях ошибок нет. Но если нас интересует не только «вычислимость», но и содержание процессов, данные о которых обрабатываются компьютерами, то оказывается, что расширенные трактовки становятся опасными. Не понимая сути, легко получить «два землекопа и две трети». Забыв о семантике, мы получили «сон разума».

Интерпретация (то есть привязка содержания к форме) полученных компьютерами чисел сегодня осуществляется программами. Или, как в случае технической задачи, которую решал непосредственно Тьюринг – внешним экспертом. Задача «не потерять физический смысл» – сверхзадача для программиста, создающего приложение. Но всегда существует предел сложности, выше которого проконтролировать семантику преобразований не в силах человека. В результате – складываем лампочки и апельсины, получаем лампольсины. Целое распадается на несвязанные цифры, глядя на которые нельзя понять, где же форма, а где содержание. Именно «лампольсины» и есть источник «успехов» хакеров. Сместить указатель машины Тьюринга, неверно интерпретировать содержимое ячейки памяти, вызвать прерывание – и подмененный обработчик передаст управление негодяю. Вот и вся схема практически любой атаки.

Можно ли что-то с этим сделать? Да. Учитывать смысл. Применять механизмы датацентричности и моделеориентированности. Не складывать яйца и помидоры. Или складывать в моделях «холодильник» и «сковорода».

Надеюсь, ассоциации понятны. Надеюсь, что скоро это будет осознанно и станет общим местом. А мы создадим семантическую безопасность.

Наука давно обратила внимание на эти проблемы. Конечно, в первую очередь это М. Минский, отец современных подходов к искусственному интеллекту, придумавший «фреймы для представления знаний» как нечто, объединяющее процедуры и данные для них, и Л. Заде, посвятивший свою жизнь созданию нечетких множеств, где количественная оценка (функция принадлежности) объединяется с семантикой (континуум) в единый синглетон. К сожалению, эти работы до сих пор не интегрированы в практику проектирования информационных систем, вычисления и их интерпретация остаются разорванными.

Как заведующий кафедрой МФТИ, что Вы считаете максимально важным для подготовки кадров в области цифровой безопасности?

Практически все готовят специалистов, знающих нормативную базу и умеющих устанавливать и настраивать СЗИ. Нет сомнения, что такие специалисты нужны. Они востребованы везде – от кредитно-финансовой сферы и промышленных предприятий до органов государственного управления.

Однако почти никто (одно из редких исключений – наша кафедра) не готовит специалистов, умеющих разрабатывать СЗИ. С учетом вопроса, на который я ответил выше, я вижу два важнейших направления – это подготовка специалистов по защите систем цифровой экономики и подготовка разработчиков СЗИ нового типа.

Освещение каких областей цифровых технологий Вы хотели бы видеть в нашем журнале?

В первую очередь – побольше нового и поменьше «правильного». Поменьше культурологической направленности (информационной безопасности), нормативных аспектов, и побольше технических решений (технической защиты информации).

В общем – все направления хороши, если изложены профессионально. Давайте сами себя избавим от дилетантских и начетнических работ и создадим журнал, который будет служить источником новых идей для нового поколения специалистов.

А читать в первую очередь я буду работы по семантической интероперабельности и связи «Смысл – безопасность». А писать – по интерактивной биометрии.

Поделитесь, пожалуйста, с нашими читателями самым веселым эпизодом из Вашей практики гуру информационной безопасности?

У нас вся жизнь – обхохочешься. Смешно,

когда примитивными приемами социальной инженерии негодяи всякого рода пытаются выманить из меня деньги. Смешно, когда для того, чтобы снять защиту, обеспечиваемую сертифицированным «Аккордом», у нас просят пароль и идентификатор от него, и еще смешнее, когда уверяют нас, что мы-то должны знать, как обойти собственную защиту.

Смешно (до слез), когда в ведомствах, ранее славившихся надежностью защиты, класс падает до потери миллионов наборов персональных данных, при одновременном росте амбиций нового поколения руководителей в области ТЗИ.

Ну а действительно смешной случай могу припомнить. Однажды я заметил, что один из хороших специалистов в нашей области в публичных дискуссиях всякий раз применяет один и тот же дидактический прием. Конструкция, казавшаяся яркой в первый раз, немного поблекла во второй, и стала совсем уж никакой на третий раз. Но тут в одной из дискуссий нам довелось встретиться на сцене. Я отношусь с большим уважением к своему коллеге, но не мог не воспользоваться случаем и перехватил инициативу, аргументируя свои мысли его конструкциями. Весело было и мне, и залу. Уж не знаю, как коллеге. Но, думаю, нас всех этот случай чему-то научил.

Хочу рассказать и о случае из далекого прошлого. В юности, чтобы получить доступ к ЭВМ, мы с моими товарищами подрядились на работу по совместительству в один из важных НИИ, изучавший предложение (!) и спрос (!) на рынке (!) СССР. Машинное время для собственных исследований нам было нужно так сильно, что мы согласились разработать программу краткосрочного прогнозирования для Брянской области.

В целом мы с задачей справились, и эта область жила не хуже других.

Однако люди моего поколения помнят, что через несколько лет в СССР исчезла посуда (появились шутки в КВН о летающих тарелках) и все магазины закупили черно-белые телевизоры. Мучаясь подозрениями, мы стали задавать осторожные вопросы, и в результате выяснилось, что систему краткосрочного прогнозирования маленькой области применили для среднесрочного прогноза огромной страны. Руководство института должно было отчитаться в срок, потому и выбрали неподходящий инструмент, провели опыты на людях.

Наверное, тогда я хорошо понял, что для решения любой задачи нужны адекватные инструменты, иначе быть беде.

Теперь я снова живу в ожидании беды, видя попытки применить биометрию, предназначенную для криминалистики, в решении задач цифровой экономики.

Валерий Аркадьевич, благодарим Вас за интересную содержательную беседу.

Беседовала Анна Глазкова