МВД России
Санкт-Петербургский университет

Факультет подготовки следственных работников

Кафедра специальных информационных технологий

Слушательское научное общество

Компьютерные технологии в экспертной деятельности

Сборник научных статей

Выпуск 2

Санкт-Петербург
2010

УДК 681/3
ББК 32.81
К63

Компьютерные технологии в экспертной деятельности: Сб. научных статей курсантов факультета подготовки следственных работников Санкт-Петербургского университета МВД России. Вып. 2. / Под науч. ред. А.А. Кабанова. – СПб.: СПб ун-т МВД России, 2010. – 28 с.

В сборник включены статьи курсантов 238 учебного взвода факультета подготовки следственных работников Санкт-Петербургского университета МВД России, обучающихся по специальности 350600 – судебная экспертиза. В сборнике кратко рассматриваются актуальные вопросы применения компьютерных технологий в экспертной деятельности, а также вопросы, непосредственно связанные с ними. Вступительная статья написана А.А. Кабановым. Замечания и предложения по сборнику просим присылать по e-mail: ***akabanov@inbox.ru.***

Редакционная коллегия: А.А. Кабанов, О.А. Кокорева,
В.В. Кутузов, О.Г. Юренков
Компьютерная верстка: А.А. Кабанов

Ген – это не что иное, как
последовательность около
3,5 миллиардов простых
органических оснований, которые
располагаются подобно ступенькам
лестницы между двумя нитями из
фосфата и сахара.
Януш Вишневский «Одиночество в Сети»

Все очень просто по сравнению с бесконечностью (вместо предисловия)

А.А. Кабанов

Килобайты, Мегабайты, Гигабайты, Террабайты, Петабайты, Экзабайты, Зеттабайты и т.д. – это всего лишь конечные величины. Информации же в мире бесконечное множество, и она бесконечно разнообразна. Однако для агностицизма нет причин. Стремление к знаниям – одна из существенных, неотъемлемых характеристик любого человека и даже любого живого существа, включая простейший вирус. Эксперты – не исключение. Большинство молодёжи, выбравшей эту профессию, способны к самостоятельной научной деятельности. Данный сборник – наглядное тому подтверждение. Не только ответы на поставленные вопросы, но и некоторые из названий статей – результат творчества его участников.

Активность в процессе обучения, поставленная целью сборника, достигнута. Авторы справились с трудной научной задачей краткого изложения нелёгких вопросов современной экспертной деятельности, и заслуживают самой высокой оценки. Это – уже второй выпуск, и, по всей видимости – не последний, причём перечень актуальных вопросов для третьего выпуска также составлен самими курсантами в процессе обсуждения изучаемых тем на практических занятиях по предмету «Компьютерные технологии в экспертной деятельности».

Так сможем ли мы своим конечным изученным количеством информации охватить всё её многообразие? Да. Надо всего лишь отделить зёрна от плевел, отбросить всё лишнее. Оставить самое главное. Процесс познания не окончен. Он продолжается. Придут за нами те, кто лучше нас.

Автоматизированное рабочее место эксперта

В.Э. Белан

Автоматизированное рабочее место (АРМ) эксперта – комплекс технических и программных средств для автоматизации профессиональной деятельности эксперта.

АРМ бывают *трёх* видов:

• *индивидуального пользования,* то есть комплекс технических и программных средств, необходимых для автоматизации деятельности одного лица (эксперта), и используемых им;

• *группового пользования.* Это такие комплексы программных и технических средств, которые могут использоваться в работе группы экспертов (коллегии), чаще всего объединённых вместе по причине их необходимости для проведения определённого рода исследования;

• *сетевые* – такие АРМ, которые подразумевают собой комплекс из рабочих мест для нескольких экспертов, работающих в единой сети и имеющих равный доступ к используемой рабочей информации, общие для сети базы данных.

Назначение АРМ эксперта: исследования разного рода объектов *в* научно-исследовательских, заводских, экспертно-криминалистических и других *лабораториях*.

Основные функции АРМ:

Общие:

• автоматизация многократно повторяющихся действий экспертов, избавление эксперта от рутинной работы;

• сокращение временных затрат на производство различного рода экспертиз.

Частные:

• получение цифровых изображений;

• обработка изображений (в том числе с использованием специализированных фильтров);

• сравнительные исследования изображений;

• подготовка и печать документов, содержащих исходные и обработанные изображения;

• хранение изображений и документов в базе данных.

Автоматизированные информационно-поисковые системы в сфере судебной экспертизы

А.В. Подстрелова

Особое место среди судебных экспертиз сегодня заняли информационные технологии. Следствием этого явились, с одной стороны, определённая трансформация экспертного исследования как процесса познания, с другой – значительное расширение его возможностей, а также повышение научной обоснованности получаемых данных. В настоящее время сложилось несколько направлений компьютеризации судебно-экспертной деятельности. Информационно-поисковая система (ИПС) «Оружие» предназначена для хранения и поиска информации по нарезному оружию. Информационно-поисковая система (ИПС) «Патрон» предназначена для хранения и поиска информации по патронам для нарезного оружия. Генератор экспертных заключений (ГЭЗ) «Клинок» предназначен для создания экспертного заключения по холодному оружию. «Арсенал» – современная мощная компьютерная система, позволяющая автоматизировать всю технологическую цепочку трасологических исследований пуль, гильз и их фрагментов: от ввода информации и создания электронной базы данных, проверок и сравнительных исследований до получения экспертного заключения. «Растр» очень удобен для подготовки экспертных заключений.

Система позволяет создавать многостраничные документы, вставлять в них исходные и обработанные изображения, использовать в качестве элементов оформления линии, выноски, прямоугольники, надписи с возможностью выбора шрифтов, настройки цвета надписи и фона, другие автоматизированные ИПС, ориентированные на информационное обеспечение различных судебно-экспертных исследований. Так, ИПС «Обувь» используется для определения характеристик подошв по их следам. Кроме автоматизированных ИПС, ориентированных на тот или иной вид экспертного исследования, ныне ведутся поисковые работы и в направлении создания автоматизированных ИПС управленческого характера.

Виды взлома компьютерных систем

В.П. Сидорова

Практически любой компьютерный взлом сводится к использованию одного из следующих способов:

1. Ввод *серийного номера (регистрационного кода)* (жарг. *серийник*) (англ. *serial number, S/n*) – взлом программы посредством введения правильного регистрационного ключа (или фразы), полученного нелегальным способом. Ключ может генерироваться на основе какой-либо информации (имени владельца программного обеспечения, характеристик аппаратной части компьютера, и т.п.), либо иметь фиксированное значение. При генерации регистрационного ключа используется алгоритм, обратный алгоритму проверки введённого регистрационного ключа в программе разработчика. *Примечание 1:* Регистрационный код может распространяться в *ключевом файле (файле лицензии)* (англ. *keyfile*), который обычно помещается в каталог с установленной программой. *Примечание 2:* Для массового взлома, зачастую, создаётся (и в дальнейшем используется) *генератор ключей* (жарг. *кейген*) (англ. *keygen* сокр. от key generator) – программа для генерации регистрационных ключей (см. выше). Данный вид взлома наиболее востребован (особенно, когда программа часто обновляется или регистрационный ключ генерируется на основе какой-то информации) и поэтому наиболее ценится. Как правило, он требует бóльшей квалификации взломщика по сравнению с другими видами взлома, но не всегда.

2. Использование *загрузчика* (жарг. *лоадер*), (англ. *loader*) – способ обходить некоторые виды защиты программного обеспечения (ПО), заключающиеся в использовании внешних систем защиты. Состоит в изменении определённых фрагментов программы в оперативной памяти сразу после её загрузки в эту память, но перед её запуском (то есть перед выполнением кода в точке входа). Применение *(бинарного) патча* (англ. *byte patch*) (часто жарг. *крэк* или *кряк* от англ. *crack*) – способ, похожий на «загрузчик», но модификация производится статически в файлах программы. Как правило, это один из самых простых и быстрых способов взлома ПО.

3. Использование *взломанной версии файла(ов)* (англ. *cracked*) – способ заключается в подмене оригинальных файлов программы файлами, которые уже взломаны.

Этот список не является исчерпывающим, а лишь обозначает наиболее часто встречающиеся способы взлома. Вид взлома чаще всего обусловлен видом защиты. Для некоторых видов защиты можно использовать разные виды взлома, для других – способ может быть единственным. Но есть способы организации защиты, взломать которые невозможно.

Информационные технологии в судебной экспертизе

А.В. Яцкова

Информационные технологии сегодня заняли особое место в судебной экспертизе. Следствием этого явились определённая трансформация экспертного исследования как процесса познания и значительное расширение его возможностей, а также повышение научной обоснованности получаемых данных. Несмотря на то, что каждая из используемых ныне методик экспертного исследования, основанная на использовании компьютеров, специфична и ориентирована на решение конкретной задачи при исследовании различных объектов, все они обладают рядом общих свойств:

1) в основе этих методик лежат такие кардинальные принципы правовой информатики, как принцип системной организации объекта познания, количественных определённостей и использования математического аппарата, функциональный и алгоритмический подход к самому процессу познания и к познаваемому объекту;

2) методологической предпосылкой являются математическое моделирование объекта и разработка (или выбор) алгоритма процесса его познания. При этом под математическим моделированием в данном случае имеется в виду более широкий класс средств познания, чем класс средств, используемых при решении чисто математических задач;

3) независимо от индивидуальных особенностей в структуре каждой из таких методик можно вычленить характерные для любой из них элементы, в частности, такие, как постановка задачи и определение цели исследования; декомпозиция общей задачи на частные подзадачи; определение конкретных средств и приёмов их реализации; собственно практическая деятельность, состоящая из определённой совокупности трудовых операций; получение результата и его оценка; принятие решения;

4) ни одна методика, основанная на использовании компьютеров, не охватывает всего процесса решения экспертной задачи. Их использование, как правило, объективизирует и автоматизирует лишь ту или иную операцию (или группу операций), которая может относиться как к самому процессу познания, так и к оценке полученных результатов. Поэтому использование компьютерных технологий ни в коем случае не исключает использования качественного подхода к объекту познания.

Информационные технологии, применяемые в баллистике

М.А. Засовенко

Информационно-поисковая система (ИПС) «Оружие» предназначена для хранения и поиска информации по нарезному оружию.

Система позволяет вводить данные по оружию, редактировать ранее введённую информацию, производить поиск по заданным условиям, а также хранить и выводить на экран графическое изображение оружия, устройство оружия и следообразующих деталей и следов, оставляемых оружием на гильзах и пулях. Для работы с системой необходимо запустить файл Oruzie.exe. После некоторого ожидания на дисплее появится основной экран. Пользователь может управлять ходом работы системы, выбирая один из возможных режимов работы ИПС, представляемых системой на каждом шаге работы в основном окне. Выбор режима в меню производится с помощью мыши. В режиме «Поиск данных» можно задать информацию, по которой в базе будут отобраны записи, удовлетворяющие заданным характеристикам.

В ИПС «Оружие» данные по каждому образцу не всегда полны, так как не вся информация есть в источниках. Это создаёт определённые проблемы при поиске. Если нет данных, удовлетворяющих заданному условию, то система сообщит об этом, после чего следует «смягчить» условия поиска, убрав то или иное условие или изменив вариант задания для поиска. После некоторого времени, необходимого системе для поиска данных, будут отображены только данные, удовлетворяющие заданному условию для просмотра данных (если поиск оказался успешным), или информация, что в базе нет данных, удовлетворяющих заданным условиям. Для того чтобы закончить работу с системой, необходимо выбрать в основном меню «Выход» или нажать кнопку выхода.

Классификация признаков в компьютерно-технической экспертизе документов

В.П. Сидорова

Документы на компьютерных носителях информации являются наиболее распространёнными объектами судебной компьютерно-технической (информационно-технологической) экспертизы. В силу этого проблемы, связанные с исследованием такого рода документов, представляют особый интерес. Анализ формы и содержания электронного и бумажного документов позволяет выделить в них несколько групп признаков, характеризующих автора и исполнителя документа, а также программно-аппаратные средства, использовавшиеся при подготовке документов. Эти признаки можно классифицировать следующим образом:

первая группа – признаки, характеризующие настройки конкретного экземпляра программного продукта, использовавшегося при составлении документа (к этой группе относятся такие признаки, как, например, значение параметра страницы «верхнее поле» или «от края до колонтитула верхнего»);

вторая группа – признаки, характеризующие содержание и построение текста документа (например, его семантика, количество строк, заголовки и т.п.);

третья группа – признаки, характеризующие навык владения компьютером у исполнителя текста (например, выбранные гарнитура и размер шрифта, использование определённых приёмов выделения абзацев в тексте и т.п.);

четвёртая группа – авторские признаки письменной речи (использование определённых лексических средств выражения мысли, количество слов в предложениях и т.д.);

пятая группа – исполнительские признаки письменной речи. К ним относятся, например, способы акцентуации (выделения), наличие и характер орфографических и пунктуационных ошибок. Последние признаки могут проявляться даже в том случае, когда использованные программные средства позволяют выявлять и исправлять такие ошибки.

В совокупности эти пять групп признаков позволяют устанавливать соответствие бумажного и электронного документов и, как следствие, делать вывод о том, что проверяемое программно-аппаратное средство использовалось для подготовки исследуемого документа. Поскольку персональный компьютер предназначен и, как правило, используется индивидуальным пользователем, авторские и исполнительские признаки могут быть объединены в единую группу признаков письменной речи.

Компьютерные технологии в криминалистической видеозаписи

М.М. Цыздоев

Современные цифровые технологии в области фиксации аудиовизуальной информации достигли такого уровня развития, что создаются предпосылки для применения этих технологий в криминалистических целях. Цифровые методы фиксации информации во многом превзошли в настоящее время аналоговые средства по качеству записи, воспроизведения и сохранения зафиксированной информации.

Применение цифровой видеозаписи для фиксации фактических сведений в криминалистике может быть реализовано при использовании в ходе следственных действий цифровой видеокамеры и портативного компьютера. Однако при использовании этих средств возникает ряд проблем, связанных с обеспечением доказательственного значения зафиксированных данных.

Проблему доказывания при использовании цифровой видеозаписи для фиксации информации в ходе следственных действий обычно связывают с возможностью изменения зафиксированных данных с помощью компьютерных технологий, что приводит к недопустимости использования этих данных в качестве доказательств в уголовном судопроизводстве.

Поэтому основное внимание в статье уделено таким методам цифровой фиксации аудиовизуальной информации, которые исключают возможность бесконтрольного субъективного вмешательства с целью изменения данных, полученных в ходе следственного действия.

Для определения возможностей и условий допустимости применения метода цифровой видеозаписи в криминалистической практике необходимо проанализировать принципы получения цифрового видеоизображения и провести сравнения с обычными (аналоговыми) методами получения видеоизображения.

Концепция соотношения в экспертном исследовании человеческого творчества и компьютерных технологий

Т.С. Семёнова

В современном мире такое понятие как творчество связано со многими сферами общественной деятельности. К числу одной из таких сфер можно отнести творчество в сфере компьютерной технологии. *Творчество есть деятельность субъектов, приводящая к созданию новых (с ранее не существовавшими отличительными характеристиками) материальных систем и процессов, которые приводят к повышению совокупного разнообразия, обеспечивающего устойчивость этого вида, и распространение его субъектов во Вселенной.* Творческой деятельностью может быть любое изобретение – устройства или технологии. И таким изобретением по праву является ЭВМ, которые сознательно используются как средство представления знаний. Однако сами ЭВМ содержат не знание, а информацию, то есть представление или модель знания. На основе этой модели пользователь воссоздаёт необходимое ему знание. Содержимое памяти ЭВМ не равносильно человеческому знанию, которое является гораздо более сложным феноменом, но может служить удобной для коммуникации моделью этого знания. Этот принцип моделирования профессиональных знаний лежит в основе экспертных систем. Поскольку экспертные системы непосредственно помогают в осуществлении интеллектуальной деятельности человека, то разработку экспертных систем часто относят к достижениям в области искусственного интеллекта. Однако многие специалисты считают экспертные системы эффективной альтернативой искусственному интеллекту, хотя в их создании использован ряд современных достижений из области искусственного интеллекта.

Подводя итог, можно отметить то, что экспертные системы не только не предполагают вытеснения человека из каких-либо интеллектуальных сфер деятельности, а наоборот, ориентируются на то, что профессиональные знания специалиста играют весомую роль в экспертных системах. Эта роль состоит в том, чтобы сделать знания одного или нескольких экспертов достоянием любого специалиста в данной области независимо от пространственно-временных ограничений. Немаловажным является и то, что, чем выше степень автоматизации экспертного исследования, тем меньше степень творческого участия эксперта, но с другой стороны при помощи автоматизации эксперт тратит меньше времени на работу и более точен в своих оценках.

Назначение компьютерно-технической экспертизы

В.П. Сидорова

При расследовании преступления в сфере компьютерной информации наиболее характерна *компьютерно-техническая экспертиза. Её проводят в целях:* воспроизведения и распечатки всей или части компьютерной информации (по определённым темам, ключевым словам и т.д.), содержащейся на машинных носителях, в том числе находящейся в нетекстовой форме (в сложных форматах: в форме языков программирования, электронных таблиц, баз данных и т.д.); восстановления компьютерной информации, ранее содержавшейся на машинных носителях, но впоследствии стертой (уничтоженной) или измененной (модифицированной) по различным причинам; установления даты и времени создания, изменения (модификации), уничтожения, либо копирования информации (документов, файлов, программ); расшифровки закодированной информации, подбора паролей и раскрытия системы защиты от несанкционированного доступа; исследования средств вычислительной техники (СВТ) и компьютерной информации на предмет наличия программно-аппаратных модулей и модификаций, приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; установления авторства, места (средства) подготовки и способа изготовления документов (файлов, программ), находящихся на магнитных носителях информации; выяснения возможных каналов утечки информации из компьютерной сети, конкретных СВТ и помещений; установления возможных несанкционированных способов доступа к охраняемой законом компьютерной информации и её носителям; выяснения технического состояния, исправности СВТ, оценки их износа, а также индивидуальных признаков адаптации СВТ под конкретного пользователя; установления уровня профессиональной подготовки отдельных лиц, проходящих по делу, в области программирования и в качестве пользователя конкретного СВТ; установления конкретных лиц, нарушивших правила эксплуатации ЭВМ, системы ЭВМ или их сети; установления причин и условий, способствующих совершению преступления в сфере компьютерной информации. До вынесения постановления о назначении экспертизы рекомендуется проконсультироваться со специалистом по поводу её целей, формулировки вопросов, характера предоставляемых материалов. Может быть назначена идентификационная и не идентификационная компьютерно-техническая экспертиза.

Новая информационная технология: «стеганографическая дактилоскопия»

Е.А. Атемасова

По результатам сравнительного анализа программных продуктов, предлагаемых рынком и распространяемых в сети Интернет, рассмотрены особенности, современные возможности и тенденции развития перспективной информационной технологии (ИТ) – «стеганографической дактилоскопии». Актуальной проблемой ИТ является задача высоконадёжной защиты информации, в частности, защиты от несанкционированного доступа к ней. От её решения зависит сегодня развитие таких сетевых технологических направлений, как электронная коммерция, электронный банк и многих других. Всё упирается в задачу идентификации личности. А лучшим биометрическим идентификатором с давних времен считался «отпечаток пальца», тем более что его может поставить даже человек, не умеющий расписаться. Достижения современных информационных технологий вдохнули новую жизнь и новое содержание в науку дактилоскопию. Дактилоскопия – изучение отпечатков пальцев или дословно: «относящийся к наблюдению за пальцами». Интеграция цифровой дактилоскопии и технологии компьютерной стеганографии позволила создать удивительный инструмент для защиты информации, цифровых документов и продуктов мультимедиа (текстовых, графических, видео- и аудиофайлов) – «стеганографическую дактилоскопию», основным назначением которой является создание идентификаторов – скрытых цифровых маркеров (СЦМ) или, как их ещё условно называют, цифровых «отпечатков пальца».

Основные задачи скрытых цифровых маркеров: исходя из решаемых задач к СЦМ предъявляются следующие основные требования: скрытность (отсутствие демаскирующих факторов); помехоустойчивость; защищённость от деструктивных воздействий третьих лиц. В последнее время СЦМ активно стали использоваться в частности для блокированиё несанкционированного доступа нелегальных Пользователей к аудио информации в сетях и на носителях.

Базовые технологии скрытых цифровых маркеров. Анализ показывает, что все современные способы цифрового маркирования используют такие методы компьютерной стеганографии, как широкополосные сигналы и элементы теории шума.

Орудия подготовки, совершения и сокрытия преступлений в сфере компьютерной информации

Т.В. Шинтяпина

Такими орудиями являются:

Средства электронно-вычислительной техники (СВТ), а именно:

- различные виды ЭВМ: персональная ЭВМ (ПЭВМ), сервер сети ЭВМ и электросвязи, аппарат сотовой электросвязи с функцией работы в сети Интернет, банкомат, контрольно-кассовая машина с блоком фискальной памяти, электронная записная книжка, электронный переводчик, графическая станция, электронный издательский комплекс и т.п.;

- периферийные устройства: видеоконтрольное устройство (дисплей, монитор), устройство управления ЭВМ (клавиатура, манипуляторы («мышь», джойстик, «шар» – трэк-болл, «световое перо», «сенсорный экран», Isopoint Control), печатающее устройство (принтер – матричный, струйный, термографический («лазерный»), графопостроитель, плоттер), устройство видео-ввода информации (сканер, цифровая фото- или видеокамера), устройство графического ввода информации (графический электронный планшет, диджитайзер), устройство работы с пластиковыми картами (импринтер, считыватель (ридер) – оптический, магнитный или электромагнитный, перкодер или программатор) и др.;

- некоторые аппаратные средства (соединительные провода, кабели, шины, шлейфы, разъёмы, COM-порты, «шнурки», устройства электропитания, аппаратные средства защиты компьютерной информации от несанкционированного доступа и т.д.);

- устройства приёма и передачи компьютерной информации (модем);

- вредоносная программа для ЭВМ: компьютерный вирус, «троянский конь» для негласного получения и копирования конфиденциальной компьютерной информации**,** крэк-программа («взломщик» кодов защиты, генератор паролей доступа, дешифратор криптографической защиты) и др.

Наиболее широко применяемым универсальным орудием совершения преступления в сфере компьютерной информации является ПК – персональный компьютер с соответствующим программным обеспечением и периферийным оборудованием.

Основные понятия информационных систем в экспертной деятельности

Е.Н. Герасимова

Информационные системы в экспертной деятельности – это одно из основных направлений научно-технического прогресса. Экспертная деятельность – это деятельность, основанная на принципах законности, соблюдения прав и свобод человека и гражданина, объективности, всесторонности и полноты исследований, проводимая с использованием современных достижений науки и техники. Компьютерная экспертиза – это специальные познания сведущего лица – эксперта, призванные решать экспертные вопросы в отношении деяний, направленных против информационной безопасности. Информационная система – взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

Для характеристики информационной системы в экспертной деятельности используются следующие понятия:

1. Элемент информационной системы – часть системы, имеющая определённое функциональное назначение. Сложные элементы систем, в свою очередь состоящие из более простых взаимосвязанных элементов, часто называют подсистемами.

2. Организация системы – внутренняя упорядоченность, согласованность взаимодействия элементов системы, проявляющаяся, в частности, в ограничении разнообразия состояний элементов в рамках системы.

3. Структура информационной системы, порядок и принципы взаимодействия элементов системы, определяющие основные свойства системы. Если отдельные элементы системы разнесены по разным уровням и внутренние связи между элементами организованы только от вышестоящих к нижестоящим уровням и наоборот, то говорят о структуре системы. Чисто иерархические структуры встречаются практически редко, поэтому, несколько расширяя это понятие, под иерархической структурой обычно понимают и такие структуры, где среди прочих связей иерархические связи имеют главенствующее значение.

4. Архитектура информационной системы совокупность свойств системы, существенных для эксперта.

5. Целостность системы – принципиальная несводимость свойств системы к сумме свойств отдельных её элементов и зависимость свойств каждого элемента от его места и функции внутри системы.

Основные понятия исследования операций

К.В. Селивановская

Операцией называется всякое мероприятие (система действий), объединённое единым замыслом и направленное к достижению какой-то цели.

Цель исследования операций – предварительное количественное обоснование оптимальных решений.

Всякий определенный выбор зависящих от нас параметров называется *решением*. *Оптимальными* называются *решения*, которые по тем или другим признакам предпочтительные других.

Параметры, совокупность которых образует решение, называются *элементами решения*.

Множеством допустимых решений называются заданные условия, которые фиксированы и не могут быть нарушены.

Показатель эффективности – количественная мера, позволяющая сравнивать разные решения по эффективности.

Все решения принимаются всегда на основе информации, которой располагает *лицо, принимающее решение (ЛПР).*

Каждая задача в своей постановке должна отражать структуру и динамику знаний ЛПР о множестве допустимых решений и о показателях эффективности.

Задача называется *статической***,** если принятие решения происходит в наперед известном и не изменяющемся информационном состоянии. Если информационное состояние в ходе принятия решения сменяют друг друга, то задача называется *динамической*.

Информационные состояния ЛПР могут по-разному характеризовать его физическое состояние:

1. Если информационное состояние состоит из единственного физического состояния, то задача называется *определённой*.

2. Если информационное состояние содержит несколько физических состояний и ЛПР, кроме их множества, знает ещё и вероятности каждого из этих физических состояний, то задача называется *стохастической* (частично неопределённой).

3. Если информационное состояние содержит несколько физических состояний, но ЛПР кроме их множества ничего не знает о вероятности каждого из этих физических состояний, то задача называется *неопределённой*.

Понятие эффективности действий при использовании компьютерных технологий

А.Г. Боголюбова

«Действие» – процесс (механический, мыслительный и т.п.), способствующий активизации знаний при решении конкретных задач.

Элементом, способствующим трансформации знаний в активные, является «действие». «Действия» могут быть механическими и мыслительными. Последние, в свою очередь, подразделяются на вычислительные, алгоритмические, логические и прочие. Причём каждая из групп включает простые и комплексные «действия».

Классификация «действий» позволяет чётко организовать процесс обучения с учётом сложности решаемых проблем.

Применение компьютерных универсальных (технологий) программ (КУП) в естественных дисциплинах воспринимается как дело неизбежное по мере компьютеризации и информатизации учебного процесса. В связи с этим эффективность применения КУП напрямую будет зависеть не только от мастерства её разработчиков, но и от её адаптированности к конкретным условиям последующего использования. Данное использование может быть совершенно различным.

Эффективность компьютерной технологии обучения во многом зависит от структурирования материала и последовательности его подачи в зависимости от уровня знаний обучаемых.

Кроме того, эффективность действий зависит и от уровня подготовленности как человека, подающего материал, так и человека, его принимающего, вне зависимости от сложности составленного материала и его переработанности для других индивидуально-развитых обучаемых.

Применение программы Adobe Photoshop в экспертной деятельности для улучшения чёткости фотоизображений

Ю.А. Кокунова

При подготовке фототаблицы к заключению эксперта размер фотографии зачастую приходится уменьшать. При уменьшении фотоснимка чёткость графики теряется, что недопустимо при иллюстрировании экспертного исследования. Поэтому очень часто перед экспертом стоит задача улучшения чёткости снимка. Используя программу Adobe Photoshop, эта процедура окажется простой и не займет много времени.

1. Открываем программу Adobe Photoshop. Для этого необходимо выполнить следующие действия: нужно выбрать Пуск → Все программы → Adobe Photoshop.

2. После того, как Фотошоп загрузится, открываем в нём фотографию, чёткость которой необходимо улучшить. Для этого можно перетащить фотоснимок в Фотошоп из окна Windows. Также можно открыть изображение традиционно с помощью меню Фотошопа: File → Open…

3. Чтобы сделать фотоизображение чётче, нужно выбрать соответствующий фильтр из главного меню Фотошопа: Filter → Sharpen → Unsharp Mask… Или же выбрать фильтр Filter → Sharpen → Smart Sharpen…

Все фильтры группы Sharpen улучшают чёткость графики, но последние два позволяют более тонко настроить чёткость. Т.е. путём передвижения ползунков фильтра можно выбрать, как сильно нужно увеличить чёткость.

4. После выбора фильтра Smart Sharpen из главного меню Фотошопа, откроется окно, в котором можно указывать настройки чёткости. При этом промежуточные результаты увеличения чёткости будут отображаться слева. Если нужный вариант настроек выбран, достаточно нажать OK, чтобы они вступили в силу.

5. Теперь достаточно сохранить обработанную фотографию и использовать её при оформлении фототаблицы.

При необходимости обработки нескольких фотографий, можно воспользоваться «горячими» клавишами Photoshop. Если один раз настроить параметры фильтра, повторно его действие для этой или любой другой фотографии можно вызвать комбинацией CTRL+F.

Проблемы компьютеризации судебной экспертизы

Д.Ю. Кувалдина

Понятием «судебная экспертиза» обозначается чрезвычайно широкий круг самых различных исследований, проводимых в тех случаях, когда при производстве предварительного следствия и судебного разбирательства необходимы специальные познания в науке и технике, чтобы выявить и познать скрытую суть явлений и вещей и дать им научное истолкование.

Особое место сегодня заняли информационные технологии. С учётом сказанного становится очевиднее важность проблемы: человек или машина. В более же широкой постановке, это проблемы определения границ, задач и условий использования компьютеров в сфере судебно-экспертной деятельности.

Центральным является вопрос о принципиальной допустимости использования ЭВМ при производстве собственно судебно-экспертных исследований и об условиях, при которых это становится возможным. Ныне не ставится вопрос (в тех случаях, когда эксперт использует компьютер как орудие труда) познал ли он механизм «исследовательской» деятельности машины. Важно другое – надёжно ли в техническом смысле работает данная машина и даёт ли она верные результаты применительно к технологии осуществляемого процесса, например, применительно к анализу количественных характеристик выделенных признаков.

Несостоятельны и утверждения, будто эксперт не может объяснить ни характер работы ЭВМ, ни принципы формирования «выводов» машины. Дело в том, что любой компьютер работает по чётким и однозначным алгоритмам, в принципиальной структуре которых может разобраться любой специалист-предметник. Если не говорить о редчайших сбоях, ЭВМ делает только то, что ей предписано человеком. Кроме того, на любой стадии исследования пользователь ЭВМ или оператор могут вывести на печать все промежуточные результаты и проверить ход анализа. Часто это не делается лишь потому, что в подобном контроле нет необходимости. Нельзя согласиться и с высказываниями о существовании неких «машинных признаков», которые якобы не соответствуют привычным экспертным признакам и поэтому «непознаваемы». По-иному решается вопрос об операторских знаниях, особенно с учётом того, что в настоящее время основным вычислительным средством для эксперта становятся персональные компьютеры, особенно мобильные. Умение работать на них, в том числе в режиме диалога, становится для эксперта обязательным.

Создание «экспертных систем»

Е.Г. Тараканова

Компьютеризация общества – одно из основных направлений научно-технического прогресса – вызвала существенные изменения в технологии разработки и использования программных средств.

Эти изменения были подготовлены всем развитием теории и практики искусственного интеллекта (ИИ).

Суть происходящих технологических изменений заключается в появлении нового класса инструментальных средств ИИ, который стал основой создания конечных программных продуктов на основе принципиально другой технологии, с новыми качественными возможностями создаваемых продуктов, эти изменения существенно повышают интеллект программ. Новые средства заменили целую технологическую цепочку, в которой между конечным пользователем и ЭВМ находилось несколько посредников.

Обычные программы имеют фиксированную последовательность шагов, определяемых программистом, и путём обработки числовой информации ищут оптимальное решение, в то время как программы ИИ, подобно человеку, пользуются для нахождения удовлетворительного решения методом проб и ошибок. При этом производится преимущественно символьная обработка содержимого базы знаний.

Различие в структуре и частоте модификаций влияет на различие технологий разработки обычных программ и программ ИИ. Все различия, приведённые для программ ИИ, в целом характерны и для экспертных систем. Таким образом, можно попытаться дать определение экспертной системы.

Экспертная система – это компьютерная программа, которая моделирует рассуждения человека-эксперта в некоторой определённой области и использует для этого базу знаний, содержащую факты и правила об этой области, и некоторую процедуру логического вывода.

Искусственный интеллект давно стал источником новых технологических приёмов, решений, которые широко вошли в практику программирования, так, в работах по искусственному интеллекту берут своё начало такие идеи, как разделение времени, обработка списков, редактирование и отладка программ в диалоговом режиме, эвристическое программирование, графический интерфейс, использование полиэкранного дисплея и манипулятора типа «мышь» и др.

Соотношение понятий информационные и компьютерные технологии

А.С. Куза;
А.А. Кабанов

Термин «технология» в словаре С.И. Ожегова трактуется как совокупность процессов обработки или переработки материалов в определённой отрасли производства, а также научное описание способов производства.

Если сравнивать понятия «информационная технология» и «компьютерная технология», то они будут соотноситься как целое и часть. Ведь если разобрать данные дефиниции, то можно в этом убедиться. Итак, начнём:

Информационная технология – совокупность методов, производственных программно-технологических средств, объединённых в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распределение информации. Информационные технологии предназначены для снижения трудоёмкости процессов использования информационных ресурсов.

Внедрение персонального компьютера в информационную сферу технологий привело к созданию нового этапа развития информационной технологии и, как его следствие, изменению её названия за счёт присоединения одного из синонимов: «новая» или «компьютерная».

Компьютерная технология – информационная технология, использующая персональные компьютеры для реализации процесса использования совокупности средств и методов сбора, обработки и передачи данных, то есть первичной информации, для получения обобщённой информации о состоянии информационного продукта. Эта технология основана не столько на информатике (ИНФОРмация+автоМАТИКА), сколько на теленетике (ИНФОРМАТИКА+СВЯЗЬ).

Исходя из всего выше изложенного подтверждается идея о соотношении двух данных дефиниций как целого и части. Ведь информационные технологии являются своеобразным начальным этапом развития компьютерных технологий, то есть компьютерные технологии являются одним из видов информационных технологий.

Специализированные компьютерные программы, используемые при производстве экспертиз

Н.В. Майорова

При производстве различных экспертиз решение большинства вопросов осуществляется в определённой последовательности по утверждённым методикам. Это позволяет автоматизировать процесс выполнения экспертных исследований. Принимая во внимание перечень основных вопросов, которые приходится решать эксперту, можно утверждать, что давно назрела необходимость в создании современных специализированных программ, используемых при производстве экспертиз и выполняющих различные функции. Рассмотрим несколько примеров.

Расчётно-текстовый редактор «AUTO-TEXT» позволяет реализовать новую компьютерную технологию производства автотехнических экспертиз. Главная цель разработки программы «AUTO-TEXT» – решение проблемы повышения качества экспертных исследований дорожно-транспортных происшествий. Разработанная программа содержит как отдельные (независимые) подпрограммы расчёта по типовым формулам, применяемым в экспертной практике, так и сложные алгоритмы, составленные из этих формул, в соответствии с типовыми методиками решения экспертных задач (анализа наездов на пешеходов и столкновений транспортных средств).

Если говорить о производстве сравнительно новой фоноскопической экспертизы (основная задача фоноскопической экспертизы – идентифицировать диктора по голосу и установить подлинность приобщённой к уголовному делу фонограммы), то в данном случае нельзя обойтись без применения новых технологий и компьютерных программ. «Sound Forge», «CoolEdit», «Wave Lab», «Spectra Lab» (данные программы позволяют визуализировать акустические сигналы) – полезны для объективного инструментального анализа речи, способны комплексно исследовать акустическое представление звуков и их слуховое восприятие.

Очевидным является использование специализированных программ в компьютерных и компьютерно-технических экспертизах. «Forensic Assistant» является первой и единственной в России программой, включающей в себя большой и уникальный комплекс возможностей, необходимых при исследовании компьютерной информации. Эта программа позволяет искать и анализировать криминалистически значимую информацию баз программ обмена сообщениями, без почтовых программ, индексных файлов ОС Windows и т.д.

Хакер, крэкер, фрикер

В.П. Сидорова

Ха́кер (от англ. *hack* – разрубать) – чрезвычайно квалифицированный специалист, человек, который понимает самые основы работы компьютерных систем и информационных технологий (ИТ). Это слово также часто употребляется для обозначения компьютерного взломщика. Иногда этот термин применяют для обозначения специалистов вообще – в том контексте, что они обладают очень детальными знаниями в каких-либо вопросах, или имеют достаточно нестандартное и конструктивное мышление.

Крэкер (жарг. *Крякер*) (англ. *cracker*) – тип компьютерного взломщика: 1. Человек, взламывающий системы защит (в частности защиты программного обеспечения). 2. Человек, который занимается созданием крэков. Результатом работы крэкера являются т.н. крэки. В абсолютном большинстве случаев крэкер не располагает исходным кодом программы, поэтому программа изучается связкой дизассемблера и отладчика, с применением специальных утилит. *Крэк* (также искажённое *кряк* и *крак*) (англ. *crack*) – программа, позволяющая осуществить взлом программного обеспечения. Как правило, крэк пригоден для массового использования. По сути, крэк является воплощением одного из видов взлома, зачастую, это обычный патч. *Запла́тка, или па́тч* (англ. *patch* /pætʃ/ – заплатка) – автоматизированное отдельно поставляемое программное средство, используемое для устранения проблем в программном обеспечении или изменения его функционала, а также сам процесс установки патча («пропатчивание»). Однако под словом «патч» чаще понимают исправление каких-то ошибок, в то время как под обновлением – улучшение функционала и добавление новых возможностей. Размер патчей может варьироваться от нескольких килобайт до сотен мегабайт.

Взломщик – это человек, который взламывает программу при помощи уже готового крэка или без такового. *Фри́кинг* (англ. *phreaking*) – сленговое выражение, означающее взлом телефонных автоматов и сетей, обычно с целью получения бесплатных звонков. Людей, специализирующихся на фрикинге, называют *фри́керами* (англ. *phreaker*). Это же название применяют к людям, использующим в своих неправомерных действиях телефон с целью оказать психологическое воздействие на конечного абонента. В последнее время под фрикингом стали подразумевать различный взлом электронных систем. Как например, системы охраны и контроля доступа. Одним из продвигающих это направление является сайт http:www.phreaker.us

Экспертные системы как прикладная область искусственного интеллекта

Е.Г. Тараканова

Экспертные системы – это яркое и быстро прогрессирующее направление в области искусственного интеллекта. *Искусственный интеллект* – сравнительно молодое научное направление, которое занимает исключительное положение. Это связано со тем, что:

- часть функций программирования в настоящее время оказалось возможным передать машине. При этом общение с машиной происходит на языке, близком к разговорному. Для этого в ЭВМ закладывают огромную базу знаний, способы решения, процедуры синтеза, программы, а также средства общения, позволяющие пользователю легко общаться с ЭВМ;

- интеллектуальные системы в настоящее время начинают занимать ведущее положение в проектировании образцов изделий. Часть изделий невозможно спроектировать без их участия.

Системы, относящиеся к системам искусственного интеллекта в настоящее время подразделяются на:

- экспертные системы. Их элементы используются в системах проектирования, диагностики, управления и играх. Они основаны на вводе знаний высококвалифицированных специалистов (экспертов) в ЭВМ и разработке специальной системы по их использованию;

- системы естественно-языкового общения;

- системы речевого общения;

- системы обработки визуальной информации. Они находят применение в обработке аэрокосмических снимков, данных, поступающих с датчиков и т.п.

Экспертная система – это набор программ или программное обеспечение, которое выполняет функции эксперта при решении какой-либо задачи в области его компетенции. Экспертные системы выдают советы, проводят анализ, выполняют классификацию, дают консультации и ставят диагноз. Они ориентированы на решение задач, обычно требующих проведения экспертизы человеком-специалистом. В отличие от машинных программ, использующий процедурный анализ, экспертные системы решают задачи в узкой предметной области на основе дедуктивных рассуждений. Главное достоинство экспертных систем – возможность накапливать знания, сохранять их длительное время, обновлять и тем самым обеспечивать относительную независимость организации от наличия в ней квалифицированных специалистов.

Перечень актуальных вопросов

(для следующего выпуска)

1. Автоматизация ведения экспертно-криминалистических коллекций и картотек.
2. Автоматизированная система «Фоторобот».
3. Автоматизированные банки данных в судебной экспертизе.
4. Автоматизированные системы дактилоскопической идентификации.
5. Возможности математического, аппаратного и программного обеспечения в решении задач судебной экспертизы.
6. Дактилодискотеки.
7. Естественно-научные методы судебно-экспертных исследований.
8. Интерпретация результатов применения естественнонаучных методов для решения задач криминалистических экспертиз.
9. Информационно-поисковые системы в судебной экспертизе.
10. Классификация компьютерных технологий в экспертной деятельности.
11. Классификация методов и технических средств в экспертных исследованиях.
12. Математические методы, используемые в судебно-экспертных исследованиях.
13. Методы и способы защиты криминалистической информации.
14. Модели предметных областей, используемых в судебной экспертизе.
15. Общая характеристика методов и технических средств в экспертных исследованиях.
16. Основные функции математического, аппаратного и программного обеспечения в решении задач судебной экспертизы.
17. Отличительные признаки экспертных систем судебной экспертизы.
18. Правила хранения информации в компьютерах.
19. Принципы поиска, хранения, обработки и передачи информации.
20. Справочно-информационные системы в экспертных исследованиях.
21. Системы поддержки принятия экспертных решений.
22. Цифровые методы обнаружения, фиксации и изъятия объектов криминалистической экспертизы.
23. Экспертные автоматизированные информационные системы.

Содержание

Составление, предисловие и
научное редактирование:
начальник кафедры специальных информационных технологий
Санкт-Петербургского университета МВД России
Кабанов Андрей Александрович,
кандидат юридических наук, доцент,
e-mail: ***akabanov@inbox.ru***

КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ЭКСПЕРТНОЙ ДЕЯТЕЛЬНОСТИ

Сборник научных статей

Выпуск 2

Печатается в авторской редакции

Подписано в печать и свет 30.03.2010 г. Формат 60×84 1/16
Печать офсетная Объём 1,75 п.л. Тираж 100 экз.

Отпечатано в ООО «Копи-Р»
190000, Санкт-Петербург, пер. Гривцова, д. 1