

МВД России
Санкт-Петербургский университет

Правовая информатика

Материалы выступлений на заседании 19 секции
21 международной конференции
«Школьная информатика и проблемы устойчивого
развития» в Санкт-Петербургском университете МВД
России 27 апреля 2002 года

Санкт-Петербург
2002

Правовая информатика: Материалы выступлений на заседании 17 секции 21 международной конференции «Школьная информатика и проблемы устойчивого развития» в Санкт-Петербургском университете МВД России. Санкт-Петербург, 27 апреля 2002 г. / Сост. А.В. Никулин; Под ред. А.А. Кабанова. – СПб.: СПб ун-т МВД России, 2002. – 156 с.

В сборник включены материалы выступлений на заседании 19 секции 21 международной конференции «Школьная информатика и проблемы устойчивого развития». Конференция проходила в Санкт-Петербурге 26-27 апреля 2002 г. под руководством профессора М.Б. Игнатьева. Секционное заседание состоялось 27 апреля 2002 г. под руководством А.А. Кабанова. Доклад «Информационная природа открытий» и выступления приводятся в материалах в алфавитном порядке. Некоторые из выступающих, подавшие материалы своих выступлений, на заседание секции прибыть не смогли по уважительным причинам. Их тезисы приведены в сборнике в неизменном виде. Тексты тех, кто смог выступить, отрецензированы авторами в соответствии со стенограммой и результатами обсуждения.

СОДЕРЖАНИЕ

Артамонов В.С., Кабанов А.А.

А существуют ли они, законы социального управления 7

Артамонов В.С., Кадулин В.Е., Фриндунбеков Г.Э.

**Безопасность банковских информационных компьютерных
сетей 9**

Артамонов В.С., Кадулин А.В.

Пути создания системы информационной безопасности 10

Бабарыкин П.В., Тихомирова М.Л.

Перехват информации 12

Багирбеков В.К.

Технология обучения – проблемы терминологии 18

Бугель Н.В.

**Основные проблемы функционирования механизма
управления органами внутренних дел 20**

Булавчик В.В., Кабанов А.А.

Априорная неопределённость в управленческих решениях . . 21

Вешкельский А.С., Сметанин Ю.В.

**Возможности математического моделирования для оценки
криминогенной обстановки в районах сверхкрупного города 23**

Гибов В.В., Гуменюк Г.Х.

**Социально-криминологические факторы дорожно-
транспортных происшествий 25**

Гуменюк Г.Х.

**Административная деликтность как элемент дорожной
обстановки 26**

Домбровская Л.А., Ловдин Ю.И.

Компьютерная преступность и компьютерная безопасность . 28

Заборский Б.В., Мороз Н.А.

Компьютер в организации и обеспечении учебно-воспитательного процесса вуза 35

Исаков С.Л., Лукин П.А.

О путях решения проблемы компьютерных преступлений в банковской сфере 39

Кабанов А.А.

Информационная природа открытий 44

Кабанов А.А., Кутузов О.В., Бугель Н.В.

Информационно–обучающие программы с использованием интернет технологий 47

Калис Е. Б., Яковлев А.Ю.

Объект и предмет неправомерного доступа к компьютерной информации 49

Киртаев А.С.

Защита информации в ходе предупреждения валютных правонарушений 53

Кожевников Г.И., Енов О.Ю.

Обеспечение безопасности сетей, связанных с INTERNET . . . 57

Кожевников Г.И., Сухогузова Е.А.

Информационное обеспечение управленческой деятельности 59

Кокорева О.А.

Государственное лицензирование в системе информационной безопасности 64

Костюк А.В.

Применение новых информационных технологий в учебно-воспитательном процессе 69

Костюк А.В., Макарова Е.А.

Структура автоматизированной системы обучения и управления кафедры 71

Кутузов О. В.

К вопросу о применении современных компьютерных технологий для морально-психологической подготовки оперативных сотрудников органов внутренних дел 74

Лопатин В.Н.

Правовые проблемы обеспечения информационной безопасности на региональном уровне 77

Михайлов В.А.

Новые горизонты виртуальных технологий 90

Михайлов В.А., Кожеевников Г.И.

Принципы обеспечения безопасности интеллектуальных объектов 91

Немцев М.В., Бугель Н.В.

Информационные войны 94

Никулин А.В., Бабарыкин П.В.

Использование современных информационных технологий в области автоматизированной оценки знаний 99

Никулин А.В., Тихомирова М.Л.

Информационная безопасность в сфере частных интересов . 101

Перфильев Л.Г., Бабарыкин П.В.

Правовая культура учащихся в области информационных отношений 104

Петров Д.А.

Правовые аспекты информационной безопасности должника в процессе по делу о банкротстве 105

Примакин А.И.

Возможности скрытой передачи служебной информации при проведении оперативных мероприятий сотрудниками органов внутренних дел 111

Саченко А.Л.

Гражданско-правовые проблемы защиты интеллектуальной собственности 118

Таратухина О.А.

Мультимедиа технологии и интерактивные модели в системе маркетинга 123

Титов В.А.

Обеспечение информационной безопасности финансово-кредитных институтов как важное направление деятельности милиции 128

Тихомирова М.Л.

Актуальные проблемы обеспечения авторских прав в цифровой среде 129

Ходюк В.И.

Органы внутренних дел и их общая характеристика 132

Ходюк В.И., Багирбеков В.К., Кокорева О.А

Виды несанкционированного доступа к средствам компьютерной техники 136

Шаповал В.А.

Современные психотехнологии и элементы психотерапии в работе преподавателя вуза 142

Шаповал В.А., Кабанов А.А.

Психодинамически ориентированный метод оценки психического здоровья и личностного развития обучающихся . 146

Ярмоленко Н.В., Медведева О.М.

Анализ функций системы управления процессом обучения . 151

Информационный материал 153

*В.С. Артамонов, д-р воен. наук, д-р техн. наук, профессор;
А.А. Кабанов, канд. юрид. наук, доцент*

А существуют ли они, законы социального управления

*Выпить с другом – это закон.
из к/ф. «Маленькая Вера»*

Всем известен первый закон Ньютона: «Если на тело не действуют никакие внешние силы, оно будет продолжать своё равномерное и прямолинейное движение». Теоретически его можно проверить, уменьшив влияние сил на тело и убедившись в более равномерном движении, однако на практике ситуаций полного отсутствия внешних сил не бывает. Если же материальное тело окажется в гипотетической ситуации, соответствующей этому закону, то мы о нём ничего и не узнаем. Второй закон физики Ньютона гласит: «Если на тело действует внешняя сила, то оно приобретает ускорение, прямо пропорциональное величине этой силы и обратно пропорциональное массе тела». Этот закон можно проверить экспериментально с большей или меньшей точностью, т.к. на любое тело действует не одна, а всегда множество сил – гравитационное притяжение, сопротивление со стороны окружающей среды, воздействие электромагнитных полей и многое другое. Третий закон Ньютона: «Сила действия всегда равна силе противодействия», – также можно проверить с некоторой точностью. Закон всемирного тяготения $F = \gamma \times M \times m / R^2$ на примере планет солнечной системы позволил вычислить гравитационную постоянную γ с практически неограниченной точностью.

В биологии известны законы генетики, в частности, для всех людей ясно, что из семечка подсолнуха яблоня не вырастет, а вырасти может только подсолнух. Причём из одного семечка в подавляющем большинстве случаев вырастет только один подсолнух (если не погибнет). Хотя при повреждении ростка в процессе регенерации из оставшихся частей могут вырасти и целые растения. Это явление в частности используется для черенкового размножения растений. Таким образом, уже в ботанике говорить об абсолютной однозначности законов можно не всегда. В зоологии также известно, что разрубленный пополам червяк способен на регенерацию не только «хвоста», но и «головы».

В социальных системах такой очевидности законов, как в физике или математике, не наблюдается. Цитата из кинофильма «Маленькая Вера», приведённая в качестве эпиграфа, воспринимается как шут-

ка. Но, даже если рассмотреть закон (Теория управления в системах военного назначения: Учебник / А.В. Боговик, С.С. Загоруйко, И.С. Ковалев и др.; Под ред. И.В. Котенко. – М.: МО, 2001. – С. 18) о зависимости войны от политических целей правительства, то не вполне понятно, какова эта зависимость (прямая или обратная, линейная, квадратичная или кубическая, как измерить цели правительства и войну). «Изучаются они, прежде всего, философией». Что ж, вспомним законы философии: «Закон единства и борьбы противоположностей», «Закон перехода количественных изменений в качественные», «Закон отрицания отрицания»... Можно ли дать им количественную оценку и вычислить коэффициенты с такой же точностью, как гравитационную постоянную, число π или постоянную Планка? Философы при этом часто укрываются за сложностью и многокритериальностью социальных законов. Они утверждают, что из этих законов есть исключения. Взять, например, экономические законы – прибавочной стоимости или максимальной прибыли.

Кибернетика по определению – это наука о наиболее общих законах управления в технических, биологических и социальных системах. Может ли эта наука похвастать такими однозначными законами, как теорема Пифагора (квадрат гипотенузы равен сумме квадратов катетов) или $2 \times 2 = 4$? Например, закон обратной связи. В системах автоматического управления апеллируют к закону отрицательной обратной связи. В социальном управлении некоторые авторы утверждают об эффективности положительной обратной связи, которая с точки зрения технической кибернетики приводит к резонансу, «разносу» и разрушению системы. Закон повышения надёжности системы посредством дублирования исполнительных элементов также не очевиден. При таком дублировании немаловажным является факт, в «холодном» или в «горячем» резерве находятся дублирующие элементы. А ведь на основании закона дублирования некоторые авторы утверждают о возможности создания надёжных систем из ненадёжных элементов. А как быть с законом Акоффа, что система должна обладать достаточным разнообразием для того, чтобы быть в состоянии адаптироваться к изменениям внешней среды?

Так существуют ли они, законы социального управления?

*В.С. Артамонов, д-р воен. наук, д-р техн. наук, профессор;
В.Е. Кадулин, д-р техн. наук, профессор;
Г.Э. Фриндунбеков*

Безопасность банковских информационных компьютерных сетей

Прогресс банковских технологий немыслим без применения совершенной компьютерной техники, так как циркуляция огромных информационных потоков, содержащих большое количество конфиденциальных сведений, является непременным условием функционирования современного банка. Практически во всех банковских учреждениях широкое применение нашли информационные компьютерные сети, или локальные вычислительные сети (ЛВС), связанные с национальными и международными глобальными информационными сетями [1].

Анализ фактов хищений, мошенничества и других видов преступлений в банковской сфере, совершаемых с использованием компьютерной техники, показывает, что 80-90% из них совершаются при прямом участии, пособничестве или попустительстве персонала, обеспечивающего работу локальных вычислительных сетей. И это вполне объяснимо. Ведь администраторы ЛВС назначаются из числа высокообразованных специалистов, имеющих соответствующий профессиональный опыт и обладающих необходимым объёмом знаний в сфере банковских технологий. Причём, как правило, эти люди работают самостоятельно, в отдельных помещениях и практически бесконтрольно.

Совокупность этих факторов создаёт почти идеальные возможности для различных злоупотреблений и мошенничества. Основываясь на ложно понимаемом принципе экономии штатных единиц, многие финансовые структуры стремятся минимизировать численность подразделений, занимающихся обслуживанием компьютерной техники и программного обеспечения. В результате каждый участок банковских технологий, а зачастую даже не один, чаще всего обслуживается только одним специалистом-компьютерщиком. В результате из перечня средств обеспечения законности операций исключается такой мощный рычаг воздействия на потенциального нарушителя, как взаимный контроль.

В настоящее время практически все банковские структуры имеют собственные службы, отделы или управления безопасности. Однако далеко не во всех имеются подразделения или хотя бы отдельные сотрудники, занимающиеся вопросами защиты информации и предотвращения злоупотреблений с применением компьютерной техники [2, 3].

Разумеется, речь здесь может идти лишь о высококвалифицированных специалистах, чья профессиональная подготовка не уступает той, которой обладают контролируемые ими администраторы.

Таким образом, для обеспечения безопасности банковских компьютерных сетей необходимо предусматривать не только меры по их защите от несанкционированного доступа внешних злоумышленников, но и от злонамеренных действий легально зарегистрированных в системе пользователей.

Литература:

1. Гайкович В., Першин А. Безопасность электронных банковских систем. М.: Компания «Единая Европа», 1994.
2. Карпов А.Г. Нормативно-правовое обеспечение защиты информации. Журнал: Защита информации «Конфидент», СПб., 1994, № 1.
3. Щербаков А. Разрушающие программные воздействия. М.: Издательство «Эдель», 1993.

*В.С. Артамонов, д-р воен. наук, д-р тех. наук, профессор;
А.В. Кадулин*

Пути создания системы информационной безопасности

Россия вступила в эру информатизации существенно позже других индустриально развитых государств, поэтому она делает первые успешные шаги на пути внедрения современных информационных технологий и решения задач правового регулирования информационных процессов в обществе. Глобализация процессов информатизации является не только благом, но и приводит к негативным социально-правовым последствиям. Доктрина информационной безопасности России, утверждённая 9 сентября 2000 года Указом Президента Российской Федерации № 1895, призвана сыграть доминирующую роль в формировании демократического и безопасного информационного пространства России [1].

При всей своей многоплановости и конкретности положений Доктрина как научная теория и руководство к построению системы информационной безопасности личности, общества и государства не обладает в полной мере системностью подхода к этой комплексной проблеме. Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на це-

ли, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Под информационной безопасностью Российской Федерации понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [1].

Только при условии понимания государством в лице органов власти своих интересов, формулирования, заявления и реализации единой государственной политики, обеспечения понимания этой политики в обществе и организации взаимодействия со всеми структурами гражданского общества и действенного контроля с их участием, можно создать как информационное общество, так и правовое государство в России [2].

Системное решение проблемы информационной безопасности может быть осуществлено при условии реализации следующих задач:

1. Одной из первоочередных задач по созданию действительно надёжной системы информационной безопасности и защиты информационного пространства России является своевременное развитие законодательства.

2. В целях конкретизации основных положений Доктрины необходимо разработать концепцию системы информационной безопасности России, к созданию которой должны быть привлечены как государственные, так и общественные институты.

3. Необходимо способствовать развитию общественных институтов в области обеспечения национальной безопасности вообще и информационной безопасности в частности. При этом взаимодействие между государством и общественными институтами должно строиться не на принципах создания оппозиционных противовесов, а в творческом содружестве, в поиске общих точек приложения усилий и всестороннем учёте сфер взаимных интересов.

4. В сфере образования Российской Федерации назрела настоятельная необходимость разработки современной комплексной программы подготовки специалистов в области обеспечения информационной безопасности [3].

Таким образом, создание действительно эффективной системы информационной безопасности России – это комплексная проблема, успешное решение которой возможно на основе кадрового обеспечения её главных компонент путём реализации соответствующей учебной подготовки, переподготовки и повышения квалификации специалистов сферы информационной безопасности, а также организации обучения населения страны.

Литература:

1. Доктрина информационной безопасности России. Утверждена Указом Президента Российской Федерации 9 сентября 2000 года № 1895.

2. Сальников В.П. Концептуальные основы обеспечения информационной безопасности Российского государства. Актуальные проблемы безопасности информационного пространства: Материалы Всероссийской научно-практической конференции. Санкт-Петербург, 5-8 октября 1999 года / Под общ. ред. В.П.Сальникова. СПб.: Санкт-Петербургский университет МВД России, 1999.

3. Кадулин В.Е. Обеспечение безопасности информации в автоматизированных системах организационного управления // Материалы международной научно-практической конференции 23-25 ноября 1994 года «Безопасность человека и преступность». СПб.: Санкт-Петербургский юридический институт МВД России, 1994.

Бабарыкин П.В.;

Тихомирова М.Л.

Перехват информации

Различают следующие виды перехвата информации:

1. Непосредственный (активный) перехват. Осуществляется с помощью непосредственного подключения к телекоммуникационному оборудованию компьютера, компьютерной системы или сети, например линии принтера или телефонному проводу канала связи, используемого для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера. В связи с этим различают:

1) форсированный перехват (wilful intercept), представляющий собой перехват сообщений, направляемых рабочим станциям (ЭВМ), имеющим неполадки в оборудовании или каналах связи;

2) перехват символов (character seize) - выделение из текста, набираемого пользователем на клавиатуре терминала, знаков, не предусмотренных стандартным кодом данной ЭВМ;

3) перехват сообщений (message wiretapping) - несанкционированное подключение специального терминала к линии связи, приём и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

Подключение осуществляется с помощью использования бытовых средств и оборудования: телефона, отрезка провода, составляющих телефонного кабеля, компьютерного полипроводного шлейфа, зажимов типа «крокодил», специальных щупов-игл от контрольно-измерительной аппаратуры (в т.ч. и для прокалывания изоляционного слоя), набора радиомонтажных инструментов, кассетного портативного магнитофона, принтера, модема, либо персонального компьютера типа «Laptop» в блокнотном и субблокнотном исполнении.

После подключения к каналу связи, вся информация записывается на физический носитель или переводится в человекочитаемую форму посредством бытовой или специальной радиоэлектронной аппаратуры. В качестве специальной аппаратуры преступниками могут использоваться:

а) компьютеризированные анализаторы проводных линий связи, обеспечивающие программируемую последовательность записи перехватываемой информации, совместимые с любой проводной телефонной системой и позволяющие одновременно прослушивать до 256 и более линий связи;

б) многофункциональный цифровой регистратор сигналов типа MSR (Multi Signal Regustrator), представляющий собой современную систему сбора и обработки телефонных и радиопереговоров, построенную на основе новейших информационных технологии — обычный персональный компьютер, реализованный на базе платформы Intel с использованием платы обработки сигналов на основе процессора ADSP с 16(32)-канальным автоматическим цифровым преобразователем и выполненный в мультимедийном конструктиве LV-8000. Интересны следующие тактико-технические данные спецкомпьютера:

- программное обеспечение работает в режиме реального времени;

- обеспечивается длительный непрерывный перехват речевой, факсимильной и цифровой информации по 4-8-16-32 каналам проводной и радиосвязи («на выбор») с последующей её автоматической фильтрацией (удалением шумов и фона), распознаванием (идентификацией голоса), обработкой и архивированием.

2. Электромагнитный (пассивный) перехват. Не все перехватывающие устройства требуют непосредственного подключения к системе. Данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых находятся средства коммуникации, а также на значительном удалении от них. Так, без прямого контакта можно зафиксировать и закрепить на физический носитель электромагнитное излучение, возникающее при функционировании многих

средств компьютерной техники, включая и средства коммуникации. Это физическое явление привлекает особо пристальное внимание специалистов различных профессий из-за всё более широкого применения компьютерных систем обработки данных. Ведь работа всех без исключения электронных устройств сопровождается электромагнитным излучением, в результате чего в различных электронных приёмных устройствах возникают нежелательные помехи.

Электронно-лучевая трубка, являющаяся центральным элементом компьютерного устройства для видеоотображения информации на экране (дисплее) излучает в окружающее пространство электромагнитные волны, несущие в себе определённую информацию, данные («электронный смог»). Волны, излучаемые этим прибором, примерно так же, как при телевизионном вещании, проникают сквозь различные физические среды с некоторым коэффициентом ослабления, например, через стекло оконных проёмов и стены строений, а принимать их можно, как показывают данные многочисленных экспериментов, на расстоянии до 1000 м. Как только эти сигналы приняты соответствующей аппаратурой и переданы на другой компьютер (преступника), можно получить изображение, идентичное изображению, возникающему на мониторе «передающего» компьютера, для чего достаточно настроиться на его конкретную индивидуальную частоту. Каждый компьютер можно идентифицировать по конкретным параметрам: рабочей частоте, интенсивности электромагнитного излучения и т.д. Так, благодаря излучению дисплейных терминалов, можно считывать с них данные при помощи различных технических средств, приобретаемых преступником, как легальным путём, так и с использованием различных способов совершения преступлений, в том числе и выделенных нами в первой группе. Например, для осуществления преступных целей иногда достаточно смонтировать приёмную антенну по типу волнового канала и имеющую более острую, чем у обычной дипольной антенны, несимметричную диаграмму направленности. После чего разработать (или использовать готовую) программу расшифровки «снятых» данных. Изготовление и подбор указанных орудий подготовки преступления могут быть осуществлены любыми лицами, имеющими средний уровень профессиональной подготовки по соответствующим специальностям.

Впервые дистанционный перехват информации с дисплея компьютера открыто был продемонстрирован в марте 1985 г. в Каннах на Международном конгрессе по вопросам безопасности ЭВМ. Сотрудник голландской телекоммуникационной компании РТТ Вим-Ван-Эк шокировал специалистов тем, что с помощью разработанного им

устройства из своего автомобиля, находящегося на улице, «снял» данные с экрана дисплея персонального компьютера, установленного на восьмом этаже здания, расположенного в ста метрах от автомобиля.

При совершении компьютерного преступления указанным способом преступниками в ходе осуществления криминальной «операции» используются приёмы и методы оперативно-розыскной деятельности, в том числе и специальная техника. Например, различные сканирующие устройства, функционирующие на базе приёмников электромагнитных сигналов типа AR-3000A, ICOM 7100/9000 и STABO XR-100 зарубежного производства, позволяющие принимать и демодулировать радиосигнал в широком диапазоне частот (стоимостью около 400 долл. США). С исследовательской точки зрения интересен тот факт, что специалистам во время практических экспериментов удавалось принимать информацию одновременно с 25 дисплейных терминалов, расположенных в непосредственной близости друг от друга и разделять (сортировать) данные, выведенные на каждый экран из общего «электронного шума». По мнению экспертов, теоретически возможно извлекать данные одновременно даже с 50 терминалов. Иногда преступники подключают к своему телевизионному приемнику видеоманитофон (в обычном бытовом или портативном варианте исполнения), который позволяет им зафиксировать и накопить необходимую информацию на физическом носителе с целью её дальнейшего анализа в стационарных условиях.

3. Аудиоперехват или снятие информации по виброакустическому каналу. Данный способ совершения преступления является наиболее опасным и достаточно распространённым. Защита от утечки информации по этому каналу очень сложна. Поэтому рассмотрим его более детально.

Этот способ съёма информации имеет две разновидности: заходовую (заносную) и беззаходовую. Первая заключается в установке инфинитивного телефона (подслушивающего устройства - «таблетки», «клопа», «жучка» и т.п.) в аппаратуру средств обработки информации, в различные технические устройства, на проводные коммуникационные линии (радио, телефон, телевизионный кабель, охранно-пожарной сигнализации, электросеть и т.п.), а также в различные конструкции инженерно-технических сооружений и бытовых предметов, находящихся на объекте с целью перехвата разговоров работающего персонала и звуковых сигналов технических устройств (определение номера вызываемого абонента АТС и т.п.). Установка «клопа» или иной разведывательной аппаратуры на объект возможна тремя способами. В первом - необходимо скрытное или легендированное проникновение в

помещение; во втором случае - радиопередающая и звукозаписывающая аппаратура устанавливается во время постройки или ремонта помещения; в третьем - приобретается или заносится самой потерпевшей стороной (монтируется в приобретаемую аппаратуру или предметы). Например, только в 1993 г. по данным отечественной фирмы «Ан-корт», специализирующейся в области защиты информации, на территории России было продано свыше 70000 специальных устройств перехвата информации зарубежного производства.

Обнаружить аппаратуру съёма информации крайне трудно и технически сложно выполнимо, так как она, обычно, очень хорошо камуфлируется преступником (под микросхему, зажигалку, булавочную головку и т.д.) и может устанавливаться как внутри зоны контролируемого помещения, так и за её пределами, а в ряде случаев - на значительном расстоянии.

Вторая — беззаходовая разновидность - наиболее опасна. Заключается она в следующем. Акустические и вибрационные датчики съёма информации устанавливаются на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого необходимо принимать речевые сигналы. Выделяют следующие типовые конструкции инженерно-технических сооружений, по которым передаются речевые сигналы: несущие стены зданий, перегородки, перекрытия, окна, оконные рамы, двери и дверные коробки, вентиляционные воздуховоды, короба коммуникационных систем, трубопроводы. При этом не обязательно проникать внутрь помещения - достаточно приблизиться к нему снаружи. Датчик устанавливается либо непосредственно, либо дистанционно. В последнем случае используются различные выстреливающие устройства и специальное автоматическое крепление (захват) для удержания датчика на конструкции.

Иногда на более высокопрофессиональном уровне преступником могут использоваться направленные спецмикрофоны и дорогостоящие лазерные устройства, предназначенные для дистанционного снятия речевой информации через открытые сквозные проёмы (двери, окна, форточки, мусоро- и воздуховоды и т.п.) и оконные (автомобильные) стекла. Естественно, что при использовании подобной аппаратуры, которая помещается в маленьком дипломате, чемодане, коробке, установка датчика на объект не требуется.

5. «Уборка мусора». Этот способ совершения преступления заключается в неправомерном использовании преступником технологических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Он осуществляется в

двух формах: физической и электронной. В первом случае поиск отходов сводится к внимательному осмотру содержимого мусорных корзин, баков, ёмкостей для технологических отходов и сбору оставленных или выброшенных физических носителей информации.

Электронный вариант требует просмотра, а иногда и последующего исследования данных, находящихся в памяти компьютера. Он основан на некоторых технологических особенностях функционирования средств компьютерной техники. Например, последние записанные данные не всегда стираются в оперативной памяти компьютерной системы после завершения работы или же преступник записывает только небольшую часть своей информации при законном доступе, а затем считывает предыдущие записи, выбирая нужные ему сведения. Последнее возможно только в тех системах, в которых не обеспечивается необходимый в таких случаях иерархический принцип защиты доступа к данным. Примечателен здесь случай из зарубежной практики, когда сотрудник службы безопасности коммерческого вычислительного центра, обслуживающего несколько крупных нефтяных компаний, находясь на своем посту в зале работы клиентов, обратил внимание на то, что у одного из клиентов, работавших на компьютере, перед тем, как загорится световой индикатор записи его информации на магнитный диск, всегда сравнительно продолжительное время горит индикатор считывания информации. Проведённой по данному факту доследственной проверкой было установлено, что клиент занимался промышленным шпионажем.

В некоторых случаях преступником могут осуществляться действия, направленные на восстановление и последующий анализ данных, содержащихся в стертых файлах. Достижение этих целей предполагает обязательное использование в качестве орудия преступления различных программных средств специального назначения, относящихся к инструментальным программным средствам. Одним из них является программный комплекс PC Tools Deluxe, содержащий универсальную программу `pc.exe`, позволяющую восстанавливать ранее стертые («уничтоженные» с точки зрения пользователя) программы и файлы, и имеющий широкое распространение в пользовательской среде. Экспериментально было установлено, что на эту операцию преступником обычно затрачивается всего несколько минут.

Отметим, что чтение информации посредством данного способа возможно в том случае, когда пользователь выключает компьютер без соответствующих действий, направленных на полное уничтожение остаточных данных.

В.К. Багирбеков, канд. пед. наук, доцент

Технология обучения – проблемы терминологии

Повышение качества профессиональной подготовки всех категорий сотрудников МВД является одним из основных направлений повышения эффективности деятельности правоохранительных органов в целом.

Существующая система подготовки будущих офицеров МВД России представляет собой систему массового обучения, которая базируется на традиционной организации учебного процесса и характеризуется: 1) обучением в учебных группах с количественным составом не менее 25-30 обучаемых, 2) лимитом учебного времени, выделенного на освоение отдельных элементов и всей программы обучения, 3) жёсткой системой планирования содержания обучения и организационных форм проведения учебных занятий. Перечисленные характеристики учебного процесса определяют необходимость организации взаимодействия обучающего и обучаемых в процессе проведения учебных занятий в рамках дидактической системы «традиционная».

Дидактическая система «традиционная» характеризуется: 1) отсутствием постоянной обратной связи с обучаемыми в процессе проведения учебного занятия, 2) невозможностью адаптации обучающей информации к специфическим индивидуальным особенностям деятельности обучаемых. В теории педагогики она отнесена к разряду систем, обладающих минимальными дидактическими возможностями. Потолок потенциальных возможностей дидактической системы «традиционная» ограничен достижением только 2 уровня усвоения (знания-знакомства и знания-копии) и не гарантирует формирование тех профессиональных умений и навыков (3 уровень усвоения), которые определяют уровень профессиональной подготовки выпускника вуза МВД РФ. Поэтому организация взаимодействия преподавателя и обучаемых в рамках дидактической системы «традиционная» не способна обеспечить достижение целей профессиональной подготовки специалистов. Для их гарантированного достижения на заключительных этапах изучения тех учебных дисциплин, которые непосредственно определяют квалификационные характеристики выпускника в отношении его функциональных обязанностей по первичной должности в ОВД и внутренних войск, должны использоваться более эффективные дидактические системы. К таким системам относятся дидактические системы «малая группа» и «репетитор».

Более высокие потенциальные дидактические возможности этих систем определяются тем, что при числе обучаемых менее 5-7 человек психофизиологические возможности человека-преподавателя обеспечивают возможность реализации постоянной обратной связи с обучаемыми. При этом односторонняя проводимость педагогического общения как единственного канала связи между обучающим и обучаемыми в процессе обучения определяет различные для этих двух дидактических систем возможности адаптации обучающей информации к потребностям обучаемых: 1) полная адаптация к специфике учебной деятельности единственного обучаемого в дидактической системе «репетитор», 2) частичная адаптация в дидактической системе «малая группа». Однако уменьшение количественного состава учебных групп само по себе не гарантирует реализации высоких потенциальных возможностей таких дидактических систем. Практическая реализация этих возможностей необходимо предполагает разработку технологии индивидуального (индивидуализированного) обучения.

Понятие «технология обучения» родилось около 30 лет назад как результат осознания того факта, что педагогические теории непосредственно не применимы на практике и не обеспечивают проектирование реального учебного процесса. Возникла настоятельная необходимость соединения теории и практики, необходимость технологизации теоретических знаний и практического опыта обучения.

Термин «технология» имеет несколько толкований. В широком смысле под технологией понимают науку о законах производства материальных благ, вкладывая в нее три основные части: идеологию, т.е. принципы производства; орудия труда, т.е. станки, машины, агрегаты; кадры, владеющие профессиональными навыками. Для конкретного производства технологию понимают в узком смысле как совокупность приемов и методов, определяющих такую последовательность действий, которая гарантирует реализацию производственного процесса и получение конечного продукта вполне определённого качества. В любой технологии выделяется методология и средства реализации. Методология технологии в общем случае включает в себя: а) декомпозицию технологизируемого процесса на отдельные взаимосвязанные и подчиненные составляющие; б) алгоритмизированную реализацию определенной последовательности этих составляющих в соответствии с целью технологии; в) детерминированность предписаний по выполнению отдельных операций и процедур, формализуемую в технологической документации. Технология как процедура получения определённого продукта должна отвечать требованиям результативности, массовости и детерминированности, т.е. всем требованиям, предъявляемым

к алгоритму по А.А. Маркову. Отсюда следует, что *технология обучения — это такое нормативное описание детерминированной совокупности приемов (способов) обучения, которое соотносено со средствами их реализации и определяет процедуру выбора обучающих воздействий, адекватных потребностям обучаемого, а на ее основе - последовательность обучающих воздействий на обучаемого, гарантирующую достижение целей обучения.*

Н.В. Бугель, д-р юрид. наук, проф.

Основные проблемы функционирования механизма управления органами внутренних дел

Одной из важных характеристик современного общественного развития является усложнение социальных явлений и процессов, что обуславливает усиление роли управления, особенно в деле охраны правопорядка и борьбы с преступностью. Поскольку борьба с антиобщественными явлениями требует комплексного подхода, она должна основываться на научной оценке многочисленных социально-экономических, правовых, организационных и иных факторов общественного развития. Эффективность управления органами внутренних дел во многом зависит от состояния механизма управления, которое представляет собой совокупность форм, методов и средств, при помощи которых осуществляется управленческая деятельность в сфере охраны правопорядка и борьбы с преступностью.

Особое место в механизме управления занимают методы, так как на их базе происходит взаимное обогащение теории и практики этого вида деятельности. Методы позволяют сформировать систему правил, приёмов и подходов при решении стоящих задач. Одновременно с этим использование систем и методов при изучении новых проблем управления позволяет увеличить знание об управлении и о закономерностях протекающих в нём процессов и явлений, и способствуя тем самым развитию теории управления.

Среди большого круга вопросов совершенствования управления органами внутренних дел самого серьёзного внимания заслуживает научная разработка проблем нормативного регулирования многообразных отношений, связанных с организацией их деятельности. Это, прежде всего, объясняется тем, что от уровня нормативного регулирования зависит эффективность функционирования системы, которая призвана решать правоохранительные задачи.

Управленческая деятельность в сфере правопорядка и борьбы с преступностью в значительной мере зависит от научной обоснованности решений, принимаемых правоохранительными органами государства. По сути, процесс выработки решений формирует фундамент обоснованности в целом. Выработка управленческих решений неразрывно связана с познанием сложного механизма взаимосвязей и взаимозависимостей самых разноплановых явлений и процессов, влияющих на состояние преступности и эффективность организации борьбы с ней. В теории и практике деятельности органов внутренних дел многоплановую совокупность социальных и других факторов, влияющих на состояние борьбы с преступностью и охрану общественного порядка, принято именовать оперативной обстановкой. Она фактически включает в себя всё многообразие сторон действительности, которые учитываются в процессе организации деятельности органов внутренних дел. Одним из мощных современных средств совершенствования изучения оперативной обстановки является моделирование. Разработка методологии моделирования явлений и процессов, влияющих на деятельность органов внутренних дел, является насущной научной проблемой. В настоящей работе исследуются лишь некоторые проблемы совершенствования управления органами внутренних дел.

В.В. Булавчик,

А.А. Кабанов, канд. юрид. наук, доцент

Априорная неопределённость в управленческих решениях

Принятие управленческих решений основано на сборе и обработке информации об окружающей среде, состоянии управляемого объекта и некоторых других факторах. При этом, как правило, решение принимается в условиях ограничений по времени и информации. Неопределённость, имеющая место при принятии каждого управленческого решения обычно объясняется тем, что не хватило времени на сбор и обработку информации.

Однако следует иметь в виду, что информация бесконечна и многогранна. Как говорил поэт Ф.Тютчев, «истина изречённая есть ложь». Хотя ложь не в смысле обмана, а в смысле неизбежного искажения в конечном объяснении бесконечной по содержанию истины. Понятие неопределённости характерно не только для социальных систем.

В ядерной физике известен принцип неопределённости Даламбера. В популярном изложении он объясняется как научно установленный факт, заключающийся в том, что произведение неопределённости (погрешности) в определении скорости (точнее импульса, т.е. произведения массы микрочастицы на вектор её скорости) на неопределённость (ошибку) в определении координаты (радиус-вектора) есть величина постоянная. Увеличение точности определения скорости обязательно ведёт к снижению точности определения пространственного положения и наоборот, увеличение точности определения координат влечёт уменьшение точности определения скорости. Таким образом, имеет место «априорная неопределённость», существование которой в ядерной физике считается научно доказанным.

В социальных системах также можно говорить об этой априорной неопределённости. Речь идёт о принципиально неустранимой неопределённости, а не о недостаточности собранной информации за имеющийся период её сбора и обработки. Эту априорную неопределённость следует иметь в виду при принятии каждого управленческого решения. Частным следствием такого вывода является известное из менеджмента положение о том, что никакая самая оптимальная стратегия не гарантирует коммерческой организации защиту от банкротства, что таких, абсолютно эффективных стратегий вовсе не существует. Действительно, в условиях непрерывного изменения внешней среды невозможно предугадать, какого именно изменения следует ожидать. Прогнозирование базируется, как правило, на предположении, что изменения имеют эволюционный характер, что, зная историю изменения той или иной характеристики, можно методом линейной экстраполяции приблизительно оценить, каким будет изменение в ближайшей перспективе. Однако некоторые характеристики иногда изменяются скачкообразно, революционно. И такие изменения характеристик чрезвычайно трудно прогнозировать.

Вывод, который следует из приведённых рассуждений, заключается в том, что любое принятое решение не следует считать безошибочным. Кроме того, в само решение следует закладывать возможность его кардинального изменения в случае резкого и неожиданного изменения обстановки. Такие действия позволят учесть априорную неопределённость в управленческих решениях и, в конечном счёте, повысят качество и эффективность управления в социальных системах.

*А.С. Вешкельский, канд. юрид. наук;
Ю.В. Сметанин, д-р техн. наук, профессор*

Возможности математического моделирования для оценки криминогенной обстановки в районах сверхкрупного города

Дальнейшее развитие математических методов анализа социально-правовых явлений связывают с понятием математического моделирования. Вместе с тем, возможности математического моделирования для обоснования принятия управленческих решений в органах внутренних дел в должной мере не используются.

В выступлении рассматриваются результаты применения математического моделирования для оценки криминогенной обстановки в районах сверхкрупного города.

Традиционными являются варианты построения математических моделей на основе теории дифференциальных уравнений, теории групп, теории вероятности, математической статистики и др.

Для оценки криминогенной обстановки в районах применена математическая модель, в основу которой положен метод группового учёта аргументов (МГУА).

Математические модели, полученные МГУА, отвечают всем требованиям, которые предъявляются к моделям, используемым для исследования как промышленных, так и социально-правовых систем оптимального управления: информативностью, адекватностью и точностью в диапазоне возможных ситуационных параметров, малым временем счёта.

Согласно МГУА решение задачи моделирования большой размерности заменяется многостадийным процессом решения большого числа простых задач аппроксимации табличных данных полиномами заданной структуры.

В качестве территории для моделирования криминогенной обстановки был выбран Санкт-Петербург с его административно-территориальным делением на 20 районов.

Базовый временной интервал был выбран равным одному календарному году, чтобы можно было пренебречь заметными в Санкт-Петербурге сезонными колебаниями уровня преступности.

Вид используемых статистических данных определялся утверждёнными МВД РФ формами учёта.

В качестве исходных данных на вход обрабатывающей программы подавались:

1. Статистические сведения (все зарегистрированные преступления), ежегодно поступающие в Штаб из ИЦ ГУВД Санкт-Петербурга и Ленинградской области.

2. Количественное выражение учтённых социально-экономических факторов (криминогенных факторов) в районах города. Отбор их был произведён на основании изучения справок, отчётов и других документов, в которых практические работники органов внутренних дел дают характеристики своим районам, проводя качественный анализ криминогенных факторов. Количество и набор характеристик, согласованные в Штабе ГУВД СПб и Ленинградской области, являются (так же, как и временной интервал) параметрами настройки обрабатывающей программы.

Таблица 1

Районы	Криминогенные потенциалы (относительные значения)					
	1994 г.	1995 г.	1996 г.	1997 г.	1998 г.	1999 г.
Адмиралтейский	0,48	0,48	0,48	0,48	0,48	0,47
Василеостровский	0,38	0,38	0,38	0,38	0,38	0,38
Выборгский	0,33	0,32	0,32	0,32	0,32	0,32
Калининский	0,31	0,31	0,31	0,31	0,31	0,30
Кировский	0,24	0,24	0,24	0,24	0,24	0,23
Колпинский	0,15	0,15	0,15	0,15	0,15	0,15
Красногвардейский	0,29	0,29	0,29	0,29	0,29	0,28
Красносельский	0,19	0,19	0,19	0,19	0,19	0,18
Кронштадский	0,06	0,06	0,06	0,06	0,06	0,06
Курортный	0,11	0,11	0,11	0,11	0,11	0,11
Ломоносовский	0,06	0,06	0,06	0,06	0,06	0,06
Московский	0,38	0,38	0,38	0,38	0,38	0,37
Невский	0,50	0,50	0,50	0,50	0,50	0,49
Павловский	0,02	0,02	0,02	0,02	0,02	0,02
Петроградский	0,28	0,28	0,28	0,28	0,28	0,28
Петродворцовый	0,11	0,11	0,11	0,11	0,11	0,11
Приморский	0,27	0,27	0,27	0,27	0,27	0,27
Пушкинский	0,12	0,12	0,12	0,12	0,12	0,12
Фрунзенский	0,25	0,25	0,25	0,25	0,25	0,24
Центральный	1,00	1,00	1,00	1,00	1,00	1,00

Вклад каждого фактора в криминогенную обстановку определяется его весом, поэтому оценка весовых множителей является наиболее значимой частью обработки исходных данных.

В результате расчетов были получены весовые множители каждого социально-экономического фактора за ряд лет (1995, 1996, 1997, 1998, 1999 годы).

Следующий этап - расчёт криминогенных потенциалов районов. Полученные весовые множители умножаются на количественное значение соответствующих им криминогенных факторов, после чего производится суммирование произведений по каждому району (см. таблицу 1).

Следующий этап – ранжирование районов по степени подверженности их тому виду преступности, который учитывался в исходных статистических данных. Для наглядности произведено нормирование по максимальному значению КПП.

Полученное ранжирование может служить основой для сравнительного анализа деятельности РУВД, для определения удельной нагрузки на сотрудников милиции, а также для прогнозирования изменения криминогенной обстановки при появлении какого-либо нового объекта в районе.

В.В. Гибов, канд. юрид. наук, доцент;

Г.Х. Гуменюк, канд. юрид. наук

Социально-криминологические факторы дорожно-транспортных происшествий

Решение проблемы обеспечения безопасности дорожного движения имеет определённые как технические, так и социальные аспекты, ибо в последние два десятилетия социально-экономический ущерб от дорожно-транспортных происшествий (ДТП) достиг катастрофических размеров. Разумеется, что как технические, так и социальные аспекты ДТП взаимообусловлены. Тем не менее, социальные начала проблем обеспечения безопасности дорожного движения играют определяющую роль. Это объясняется тем, что в ДТП погибают и получают ранения люди, происходит повреждение личного, общественного и государственного имущества, и, самое главное, что центральным звеном в системе «человек – дорога» является человек.

Социально-криминологические исследования, проведённые зарубежными учёными, дают возможность осознать многочисленные

причинно-следственные связи, возникающие в дорожно-транспортных происшествиях в зависимости от личностных свойств водителей (пол, возраст, водительский стаж и т.д.), от влияния общественных факторов (коллектив, окружение, семья и т.п.). Среди других обстоятельств отмечается телосложение водителя, его заработок, семейное положение, цели поездок, взаимоотношение детей и родителей и т.д. и т.п.

Со всей очевидностью на основе изложенного следует признать важность социального аспекта в решении проблем обеспечения безопасности дорожного движения, а также и то, что предупреждение таких происшествий предполагает комплексное решение социальных, экономических, организационных и правовых проблем.

По нашему мнению при рассмотрении причин аварийности на транспорте и условий, способствующих их возникновению, необходимо исходить из ряда обстоятельств. В частности, аварийность, прежде всего, является результатом неосторожных преступлений, административных проступков и невиновных дорожно-транспортных происшествий, а также имеющуюся сложность нахождения границ причин и условий преступности в целом и неосторожной преступности в частности.

Г.Х. Гуменюк, канд. юрид. наук

Административная деликтность как элемент дорожной обстановки

В настоящий период времени в силу создавшихся объективных условий всё больше и больше формируется необходимость научного осмысления вопросов административной деликтности как наиболее важного элемента дорожной обстановки. Дорожная обстановка с точки зрения административной деликтности выражает содержание управленческой деятельности ГИБДД и выступает мерилем оценки её работы. Кроме того, она по нашему мнению в рассматриваемом контексте не получила должного юридического определения, неоднозначно трактуется как юридической доктриной, так и практическими работниками.

Среди принципиальных положений, касающихся указанной проблематики, следует выделить следующее:

– наиболее плодотворным представляется системный подход к понятию «дорожная обстановка», включающий в качестве равнознач-

ных детерминант внутриорганизационные и внешние аспекты его содержания в их взаимосвязи и развитии;

- дорожная обстановка в наиболее общем понимании означает наиболее значимые для ГИБДД условия их функционирования;

- административные правонарушения на дорогах в силу своей массовости не только в значительной мере создают фон для совершения правонарушений, не только представляют интерес сами по себе как самостоятельное явление, но, в конечном счете, способны выступать фактором, формирующим общественное мнение о состоянии правопорядка и работе ГИБДД в каждом конкретном регионе;

- включение административных деликтов в структуру дорожной обстановки позволит перейти от её количественных характеристик к качественным параметрам. Отдельные изменения в показателях, характеризующих линию деятельности ГИБДД, не могут служить единственным, а тем более объективным обоснованием оздоровления или ухудшения дорожной обстановки.

На наш взгляд дорожная обстановка в широком понимании включает в себя всю совокупность факторов, имеющих значение и влияющих в конкретном регионе в определённые временные отрезки на процесс осуществления ГИБДД задач по обеспечению личной безопасности участников дорожного движения по предупреждению и пресечению, а также раскрытию различных видов преступлений и административных правонарушений. При этом дорожная обстановка выступает в качестве объективного начала, т.к. она существует вне зависимости от нашего желания. Тем не менее, её содержание определяется воздействием субъективных свойств тех или иных лиц, являющихся как участниками дорожного движения, так и лицами, занимающимися управленческой деятельностью.

В этой связи возникает научная и практическая необходимость изучения в широком плане всей совокупности факторологических начал, имеющих непосредственное или опосредованное влияние на обеспечение безопасности дорожного движения.

*Л.А. Домбровская, канд. пед. наук, доцент;
Ю.И. Ловдин*

Компьютерная преступность и компьютерная безопасность

Изменения, происходящие в экономической жизни России – создание финансово-кредитной системы, предприятий различных форм собственности и т.п. – оказывают существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность – государственная, поэтому информация и секреты были тоже только государственные, которые охранялись мощными спецслужбами.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего вычислительных систем. Это даёт основание поставить проблему компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов совершения компьютерных преступлений.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, а также программное обеспечение и базы данных, для которых технические средства являются окружением.

В этом смысле компьютер может выступать и как предмет посягательств, и как его инструмент. Если разделять два последних понятия, то термин компьютерное преступление как юридическая категория не имеет особого смысла. Если компьютер – только объект посягательства, то квалификация правонарушения может быть произведена по существующим нормам права. Если же – только инструмент, то достаточен только такой признак, как «применение технических средств». Возможно объединение указанных понятий, когда компьютер одновременно и инструмент и предмет. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то этот факт можно квалифицировать как преступление. Так же, если с данным фактом связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность прямо предусмотрена в соответствии с законами РФ.

Каждый сбой работы компьютерной сети это не только «моральный» ущерб для работников предприятия и сетевых админи-

страторов. По мере развития технологий платежей электронных, «бесбумажного» документооборота и других, серьезный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем современной информатики. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

целостность данных – защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;

конфиденциальность информации и, одновременно, её доступность для всех авторизованных пользователей.

Следует также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надёжности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

Компьютерная преступность

Ни в одном из уголовных кодексов стран СНГ не удастся найти главу под названием «Компьютерные преступления»¹. Таким образом, компьютерных преступлений, как преступлений специфических в юридическом смысле не существует. В литературе до настоящего времени ведётся полемика о том, какие действия относить к разряду компьютерных преступлений. Сложность решения вопроса заключается также и в том, что диапазон противоправных действий, совершаемых с использованием средств компьютерной техники, чрезвычайно широк – от преступлений традиционного типа до требующих высокой математической и технической подготовки.

Попытаемся кратко обрисовать явление, которое как социологическая категория получила название «компьютерная преступность». Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

¹ Глава 28 УК РФ называется «Преступления в сфере компьютерной информации» и включает статьи № 272-274 (Прим. редактора).

Перечислим основные виды преступлений, связанных с вмешательством в работу компьютеров.

1. Несанкционированный доступ к информации, хранящейся в компьютере. Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры, «электронные корсары», «компьютерные пираты» - так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая на удачу один номер за другим, они терпеливо дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приёмнику сигналов в собственной ЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем, часто банальны), то можно внедриться в чужую компьютерную систему.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы, ошибок в программах, уязвимых мест в электронных цепях. Однажды обнаружив их, нарушитель может, не спеша, исследовать содержащуюся в системе информацию, копировать её, возвращаться к ней много раз, как покупатель рассматривает товары на витрине.

Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами идентификации и аутентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приёма. Самый простейший путь его осуществления – получить коды и другие идентифицирующие шифры законных пользователей.

Иногда случается, как, например, с ошибочными телефонными звонками, что пользователь с удалённого терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определённого времени и таким образом получить некоторую информацию, в частности коды.

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, своеобразный аналог приспособ-

соблений, помещаемых в транспорте под надписью «разбить стекло в случае аварии». Такая программа – мощный и опасный инструмент в руках злоумышленника.

Несанкционированный доступ может осуществляться в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Всё происходит так словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить всё, что в них хранится.

2. Ввод в программное обеспечение «логических бомб», которые «срабатывают» при выполнении определённых условий и частично или полностью выводят из строя компьютерную систему.

«Временная бомба» – разновидность «логической бомбы», которая «срабатывает» по достижении определённого момента времени.

Способ «троянский конь» состоит в тайном введении в чужую программу таких команд, которые позволяют осуществлять новые, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому «троянский конь» из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Есть ещё одна разновидность «троянского коня». Её особенность состоит в том, что в безобидно выглядящий кусок программы вставляются не команды, собственно выполняющие «грязную» работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т.д. (сколько угодно большое число раз), создающие «троянского коня».

3. Разработка и распространение компьютерных вирусов.

«Троянские кони» типа «сотри все данные этой программы, перейди в следующую и сделай то же самое» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко использу-

ется в комбинации с «логической бомбой» или «временной бомбой». Вирус «наблюдает» за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Всё происходит так, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека.

Начиная действовать (перехватывать управление), вирус даёт команду компьютеру, чтобы тот записал заражённую версию программы. После этого он возвращает программе управление. Пользователь ничего не заметит, так как его компьютер находится в состоянии «здорового носителя вируса». Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер «заболевает».

Среди большого разнообразия можно выделить две разновидности вирусов, обнаружение которых различно по сложности: «вульгарный вирус» и «раздробленный вирус». Программа «вульгарного вируса» написана единым блоком, и при возникновении подозрений в заражении ЭВМ эксперты могут обнаружить её в самом начале эпидемии (размножения). Эта операция требует, однако, крайне тщательного анализа всей совокупности операционной системы ЭВМ. Программа «раздробленного вируса» разделена на части, на первый взгляд, не имеющие между собой связи. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать и, следовательно, размножить вирус. Таким образом, он почти все время находится в «распределённом» состоянии, лишь на короткое время своей работы, собираясь в единое целое. Как правило, создатели вируса указывают ему число репродукций, по достижении которого он становится агрессивным.

Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер.

По-видимому, в будущем будут появляться принципиально новые виды вирусов. Например, можно себе представить (пока подобных сообщений не было) своего рода «троянского коня» вирусного типа в электронных цепях. В самом деле, пока речь идёт только о заражении компьютеров. А почему бы – не микросхем? Ведь они становятся всё более мощными и превращаются в подобие ЭВМ. И их необходимо программировать. Конечно, ничто не может непосредственно «заразить» микросхему. Но ведь можно заразить компьютер, используемый как программатор для тысячи микросхем.

Естественно, что против вирусов были приняты чрезвычайные меры, приведшие к созданию текстовых программ-антивирусов. За-

щитные программы подразделяются на три вида: фильтрующие (препятствующие проникновению вируса), противоинфекционные (постоянно контролирующие процессы в системе) и противовирусные (настроенные на выявление отдельных вирусов).

Однако развитие этих программ пока не успевает за развитием компьютерной эпидемии.

Заметим, что пожелание ограничить использование непроверенного программного обеспечения, скорее всего, так и останется практически невыполнимым. Это связано с тем, что фирменные программы на «стерильных» носителях стоят немалых денег в валюте. Поэтому избежать их неконтролируемого копирования почти невозможно.

4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям.

Проблема неосторожности в области компьютерной техники сродни неосторожной вине при использовании любого другого вида техники, транспорта и т.п.

Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надёжности, то в области программирования такая надёжность весьма условна, а в ряде случаев почти не достижима.

5. Подделка компьютерной информации.

По-видимому, этот вид компьютерной преступности является одним из наиболее «свежих». Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик, причём имеющий достаточно высокую квалификацию.

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удаётся сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосования, референдумов и т.п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы.

Естественно, что подделка информации может преследовать и другие цели.

6. Хищение компьютерной информации.

Если «обычные» хищения подпадают под действие существующего уголовного закона, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путём несанкционированного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изъятием ценностей из фондов организации. Не очень далека от истины шутка, что у нас программное обеспечение распространяется только путём краж и обмена краденым. При неправомерном обращении в компьютерную систему машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны¹.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является «средством» достижения цели. Здесь можно выделить разработку сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными – рекомендации по выбору оптимального варианта действий преступника.

Другой вид преступлений с использованием компьютеров получил название «воздушный змей».

В простейшем случае требуется открыть в двух банках по небольшому счёту. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так, чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз («воздушный змей» поднимается всё выше и выше) до тех пор, пока на счёте не оказывается приличная сумма (фактически она постоянно «перескакивает» с одного счёта на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счёта исчезает. Этот способ требует очень точного расчёта, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Можно представить себе создание специализированного компьютера-шпиона, который, будучи подключён к разведываемой сети,

¹ См. предыдущее примечание редактора.

генерирует всевозможные запросы, фиксирует и анализирует полученные ответы. Поставить преграду перед таким хакером практически невозможно. Не трудно предположить, что организованная преступность давно приняла на вооружение вычислительную технику.

Уровень компьютерной преступности определяется во многом объективными причинами и напрямую зависит от общего уровня информатизации общества. На современном этапе развития информационных технологий в России назрела необходимость детального изучения проблемы криминалистического исследования компьютерной преступности. Следует отметить, что при совершении компьютерных преступлений, также как и при совершении любых других общеизвестных видов преступлений, остаются «следы», обнаружение, фиксация и исследование которых является неременным условием как при расследовании и раскрытии данного вида преступлений, так и в борьбе с «техногенной» преступностью в целом.

Литература:

1. Рааб М. (M. Raab). Защита сетей: наконец-то в центре внимания // Компьютеруорлд, Москва, 1994, № 29, с. 18.
2. Сухова С.В. Система безопасности NetWare // «Сети», 1995, №4, с. 60-70.
3. Беляев В. Безопасность в распределительных системах. // Открытые системы. Москва, 1995, № 3, с. 36-40.
4. Ведеев Д. Защита данных в компьютерных сетях // Открытые системы. Москва, 1995, № 3, с. 12-18.

*Б. В. Заборский, канд. техн. наук, доцент;
Н. А. Мороз*

Компьютер в организации и обеспечении учебно-воспитательного процесса вуза

За последнее время произошло коренное изменение роли и места персонального компьютера и информационных технологий в жизни общества. Из предмета деятельности достаточно узкого круга специалистов в области точных наук они превратились в инструмент, используемый во всех отраслях современного производства, в быту и общественной жизни. Владение информационными технологиями ставится в современном мире в один ряд с такими качествами, как умение читать и писать. Очевидно, что в ближайшее десятилетие роль персо-

нального компьютера будет возрастать и, в соответствии с этим, будут возрастать требования к компьютерной грамотности.

Стремительная автоматизация человеческого общества неизбежно влечёт за собой утверждение новых образовательных стандартов, внедрение современных технологий в сферу образования. Использование новых информационных технологий даёт принципиально новые возможности для совершенствования педагогического процесса и повышения на этой базе образовательного уровня подрастающего поколения.

Информатизация системы образования предполагает:

- повышение уровня подготовки учащихся в области современных информационных технологий;
- разработку и внедрение информационных образовательных технологий в практику работы учреждений в сфере образования;
- создание необходимой материально-технической базы для использования информационных образовательных технологий;
- повышение эффективности образовательного процесса и работы педагогов, существенное улучшение на этой базе качества обучения и воспитания;
- создание системы информационного обеспечения управленческой деятельности в системе образования.

Сегодня специалист с высшим образованием должен свободно ориентироваться в мировом информационном пространстве, иметь необходимые знания и навыки для того, чтобы осуществить поиск, обработку и хранение информации, используя современные информационные технологии, компьютерные коммуникации и системы.

Военное образование является органической частью государственной системы образования России.

Теория и практика свидетельствуют, что образование в силу объективных и субъективных обстоятельств, а военное в особенности, относится к числу наиболее консервативных систем с точки зрения восприимчивости к нововведениям.

Высшая военная школа оказалась сегодня в ещё более сложном положении, чем гражданская, поскольку на определённом этапе её развития ей отводилась заведомо второстепенная роль.

Применение компьютера в организации и обеспечении учебно-воспитательного процесса вуза можно условно разделить на два этапа.

I ЭТАП

Изначально применение компьютера и новых информационных технологий осуществляется на занятиях по информатике.

До поступления в высшее учебное заведение у обучаемых должны быть сформированы основные знания и умения работы с информацией, в том числе и с использованием компьютера. К сожалению, нужно отметить различную школьную подготовку курсантов.

На начальном этапе происходит знакомство с архитектурой современных вычислительных систем, принципами хранения, поиска и обработки информации в компьютерных системах, основами компьютерного моделирования объектов, процессов и явлений.

Основной задачей является формирование практических навыков работы с информацией, извлечение из неё знаний с использованием методов формальной логики и систематизации их в виде баз данных и баз знаний, а также изучение элементов искусственного интеллекта с последующим их использованием при решении задач эвристическим методом. Для этого необходимо обучать курсантов методам создания баз данных с использованием систем управления базами данных, формальному описанию предметных областей (созданию баз знаний) и решению задач эвристическим методом с использованием языка логического программирования, а также автоматизации процесса вычислений с использованием электронных таблиц. Т.е. основные усилия направлены на приобретение навыков работы с прикладными программами. Для этого подходят интегрированные оболочки, которые содержат в своём составе основные компоненты автоматизации работы с информацией: текстовый редактор, электронные таблицы, системы управления базами данных и др.

При этом, несмотря на явно «пользовательскую» направленность, серьёзное внимание необходимо уделять тем направлениям информатики, которые носят базовый образовательный характер (алгоритмизация, программирование, методы формализации информации).

Изучение курса предполагает выработку у обучаемых знаний и умений, необходимых для практической деятельности по сбору, хранению, систематизации, преобразованию и обработке информации, а также решению задач с использованием алгоритмического и эвристического подходов. Здесь вычислительная техника выступает в качестве средства автоматизации работы с информацией.

Курс информатики должен взять на себя определённые функции по отработке вычислительных навыков, решению задач прикладного характера из курса математики, дисциплин кафедр тактики, тактической подготовки внутренних войск, огневой подготовки, автомобилей, бронетанкового вооружения и техники. Специфические умения и навыки работы с информацией, а также логика мышления, формируемые у обучаемых в процессе изучения информатики, дисциплинируют

их мышление, приучают ясно, исчерпывающе и лаконично излагать свои мысли и предложения, чётко и грамотно оформлять свои математические записи с использованием правил и грамматики различных языков (русского, математического, алгоритмического и символического программирования и др.).

Таким образом, информационная грамотность – это совокупность знаний, умений, навыков, овладение которыми позволит подготовить обучаемых к работе с информацией, в том числе и с применением компьютера в будущей практической деятельности.

Из выше сказанного следует, что предмет информатики может принять логически осмысленный, теоретический и практический общеобразовательный характер, направленный на систематическое развитие общих умственных способностей человека и подготавливающий его к эффективному изучению других предметов.

Целесообразно использовать информатику как основу для определения межпредметных связей.

II ЭТАП

Этот этап характеризуется применением компьютера и новых информационных технологий при изучении дисциплин специальности и специализации, выполнении курсовых и дипломных работ.

Здесь используются ранее изученные на занятиях по информатике прикладные программы, методы математического моделирования, информационные ресурсы Интернет и др.

Кроме этого, достаточно эффективным средством обучения является использование электронных учебных пособий. В библиотеке института можно создать сервер, обеспечивающий сетевой доступ учебных классов к электронным учебникам и мультимедийным продуктам.

Выполнение всех задач, поставленных на первом и втором этапах, целиком зависит от правильности разработки учебных планов и программ обучения в области информатизации, а также от правильной подготовки умений педагога использовать компьютер в преподавании своего предмета, и, конечно, для этого необходимо наличие современной технической базы.

Грамотное использование компьютера и информационных технологий на каждом этапе, а также устранение всех недостатков (отсутствие технической базы, неумение педагога применять вычислительную технику в преподавании своего предмета и др.) позволит обеспечить подготовку высокопрофессиональных специалистов, которым характерны:

системный подход к самым различным явлениям и процессам;

адекватный современному обществу стиль мышления;
информационная культура, которая должна быть присуща человеку XXI века.

С. Л. Исаков, канд. техн. наук, доцент;

П. А. Лукин

О путях решения проблемы компьютерных преступлений в банковской сфере

Важность роли, которую играет банковская система в жизни современного общества, неоспорима. Построенная на базе передовых технологий, она является важнейшим элементом экономической структуры государства. «Банки — одно из центральных звеньев системы рыночных структур. Развитие их деятельности — необходимое условие реального создания рыночного механизма».

Развитие банковских технологий немыслимо без применения совершенной компьютерной техники, так как циркуляция огромных информационных потоков, содержащих большое количество конфиденциальных сведений, является неперенным условием функционирования современного банка. Практически во всех банковских учреждениях широкое применение нашли локальные, а порой и глобальные компьютерные сети. Персональные компьютеры используются в качестве автоматизированных рабочих мест (АРМ) операторов при работе с клиентами — физическими и юридическими лицами, для обслуживания счетов и ведения внутрибанковских расчётов в составе интегрированных банковских сетей, а также совместно с телекоммуникационными системами для обслуживания удаленных клиентов в системе «Клиент—Банк».

Кроме того, компьютеры используются для проведения межбанковских расчётов в глобальных телекоммуникационных сетях и системах «Телекс», «Спринт», «Свифт», Internet и других.

Банк является кредитно-финансовым учреждением и осуществляет операции с денежными средствами, доверенными ему вкладчиками. Сохранить доверия клиентов — основная задача любого банка, а это невозможно без гарантий сохранения в тайне сведений о клиентах и их вкладах.

В условиях, когда в процесс создания, обработки, хранения и передачи банковской информации вовлечено большое количество людей и разнообразных технических средств, создание системы защиты

банковской информации и информации клиентов банка представляет собой весьма сложную организационно-техническую задачу. По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации уязвимость последней повышается, чему способствует целый ряд факторов.

Резко увеличивается объём информации, обрабатываемой с помощью персональных компьютеров (ПК) и других средств автоматизации. В единых базах данных сосредотачивается информация различного назначения и различной принадлежности. Существенно расширяется круг пользователей, имеющих непосредственный доступ к ресурсам вычислительной системы и находящимся в ней массивам данных. Усложняются режимы функционирования технических средств локальных вычислительных сетей, широко внедряются многоплатформенный и многопрограммный режимы, а также режимы разделённого и реального времени. Происходит автоматизация машинного обмена информацией, в том числе и на больших расстояниях.

В деле автоматизации банковских технологий и процессов огромная роль принадлежит локальным вычислительным сетям (ЛВС). Можно смело утверждать, что без их использования функционирование современных банковских структур просто невозможно. И здесь на первый план выходит фигура администратора ЛВС или администратора банковского сервера или сервера приложений.

Анализ случаев хищений, мошенничества и преступлений в банковской сфере, совершённых с использованием компьютерной техники, показывает, что 80-90 % из них совершаются при прямом участии, пособничестве или попустительстве именно этой категории персонала. И это вполне объяснимо. Ведь администраторы ЛВС назначаются из числа наиболее грамотных, высокообразованных специалистов, имеющих соответствующий профессиональный опыт и обладающих значительным объёмом знаний в сфере банковских технологий. Причем, как правило, эти люди работают самостоятельно, в отдельных помещениях и практически бесконтрольно.

Совокупность этих факторов создаёт почти идеальные возможности для различных злоупотреблений и мошенничества. Основываясь на ложно понимаемом принципе экономии штатных единиц, многие финансовые структуры стремятся минимизировать численность подразделений, занимающихся обслуживанием компьютерной техники и программного обеспечения. В результате каждый участок банковских технологий, а зачастую даже не один, чаще всего обслуживается только одним специалистом-компьютерщиком. В результате из перечня средств обеспечения законности операций изымается такой мощный

рычаг воздействия на потенциального нарушителя, как взаимный контроль.

Здесь уместно привести положительный пример Сберегательно-го банка. В качестве основного принципа в нём принята практика, когда ни одна операция не производится единолично и не обходится без последующего контроля другим подразделением.

Разумеется, соблюдение этого правила влечёт за собой содержание достаточно солидной штатной структуры, но получаемая взамен мощная система взаимного контроля и проверки позволяет предотвращать большую часть нарушений и оперативно обнаруживать практически все из немногих происшедших.

Вместе с тем, нельзя сказать, что столь же хорошо обстоит дело с контролем деятельности администраторов ЛВС и расчётных систем. Во многих случаях приходится полагаться на их честность и порядочность, а в условиях современной кризисной ситуации, падения уровня жизни, усиливающейся криминализации общества и пристального внимания преступного мира именно к кредитно-финансовым учреждениям эти положительные качества могут и не «сработать».

С учётом изложенного в ряду мероприятий, направленных на обеспечение безопасности банковских операций, на первый план выходят методы объективного, автоматизированного контроля деятельности администраторов ЛВС и систем.

В настоящее время практически все банковские структуры имеют собственные службы, отделы или управления безопасности. Однако далеко не во всех имеются подразделения или хотя бы отдельные сотрудники, занимающиеся вопросами защиты информации и предотвращения злоупотреблений с применением компьютерной техники.

Разумеется, речь здесь может идти лишь о высококвалифицированных специалистах, чья профессиональная подготовка как минимум не уступает той, которой обладают контролируемые ими администраторы.

Исходя из размеров потенциального материального ущерба, наибольшая опасность может исходить от администраторов баз данных платёжных систем. Они, как правило, имеют неограниченный доступ к базе данных, легко могут производить в ней любые изменения, уничтожая их в течение того же операционного дня, то есть до начала архивирования информации. За это время ложные проводки попадают в расчётные системы и могут быть обналичены сообщниками либо самим администратором.

Конечно, существует система аутентификации проводок и изменений, но опытному администратору не составит большого труда её обойти или деактивировать. Основная проблема состоит в том, что сервер отдается администратору в полное распоряжение, он получает неограниченный доступ ко всем его ресурсам. И вот здесь-то и должна быть построена ещё одна «линия обороны» – программное обеспечение, регистрирующее действия администратора и немедленно или с заданной дискретностью передающее оповещение обо всех изменениях на контрольную рабочую станцию специалиста по защите информации.

Поскольку данное программное обеспечение (агент) должно быть установлено и на сервере, то есть в доступном для контролируемого администратора месте, необходимо принять специальные меры по предотвращению несанкционированного вмешательства в работу этой программы.

Одним из способов достижения этой цели является систематическая посылка установленным на сервере программным агентом неповторяющихся зашифрованных сигналов на контрольную рабочую станцию. Сигналы выдаются только после проверки целостности кода самого агента и передачи им необходимой информации на контрольную станцию. Отсутствие специального сигнала в течение заданного интервала времени является признаком несанкционированных действий контролируемого администратора.

Информация, передаваемая на контрольную станцию с сервера, должна содержать лог-файлы операционной системы, в которых фиксируются действия любых пользователей (в том числе и администраторов), данные о любых изменениях прав доступа пользователей (в том числе и администраторов) к ресурсам системы, сведения о вводе и удалении пользователей системы, предоставлении ресурсов серверов и сетей в совместное пользование, данные о регистрации пользователей в системе и т.д.

Подобных систем контроля довольно много, и в тестировании двух из них одному из авторов удалось принять участие: системы аудита безопасности серверных платформ Enterprise Security Manager и системы мониторинга безопасности серверных платформ в реальном масштабе времени Intruder Alert, разработанных американской фирмой Axent Technologies Inc.

Системы состоят из двух частей: менеджера, устанавливаемого на контрольной станции, и агентов, которые размещаются на контролируемых серверах. Первая из них обеспечивает сбор и анализ на контрольной рабочей станции создаваемых агентами лог-файлов серверов,

а также анализ соответствия конфигурации серверов и рабочих станций сети заданной политике безопасности. Кроме того, в Enterprise Security Manager заложено множество известных на данный момент уязвимостей операционных систем, что позволяет своевременно обнаруживать их на серверах сети и выдавать рекомендации по устранению.

К недостаткам продукта можно отнести хранение в открытом виде в директориях системы ESM данных о её конфигурации, о политиках безопасности, о проверяемых файлах и их атрибутах, что делает эту информацию доступной для модификации пользователем с привилегиями администратора. Кроме того, не вполне корректна поддержка русского языка, а остановка агента не всегда своевременно обнаруживается администратором сервера из-за не совсем чёткого контроля деятельности установленных на серверах агентов программным обеспечением менеджера.

Система Intruder Alert позволяет с помощью агентов передавать менеджеру лог-файлы контролируемых серверов, оповещать обо всех заранее заданных событиях, например об изменении уровней доступа, вводе и исключении пользователей и т.д. Встроенные политики безопасности позволяют определить состояние системы не только из журналов аудита, но и средствами самого агента.

При этом продукт обладает недостаточными возможностями диагностики функционирования агентов и малым набором команд для управления ими. Регистрация событий безопасности Агентом ИТА зависит от настроек системы аудита Windows NT, изменение которых может снизить степень обеспечения безопасности, а выведение из строя системы аудита и вовсе может привести к деактивации системы мониторинга безопасности ИТА. Во время бездействия агент не регистрирует текущие события, а менеджер не выдает сообщения о недоступности агента. Принимая во внимание, что сервисы агентов могут быть остановлены пользователями с привилегиями администратора, возможно преднамеренное сокрытие некоторых действий последних.

Системы Enterprise Security Manager и Intruder Alert взаимно дополняют друг друга и для построения эффективной системы безопасности должны использоваться совместно. Предусмотренные в них эталонные политики безопасности охватывают многие методы атак на компьютерные сети как извне, так и изнутри.

Описанные в материалах выступления принципы и правила обеспечения контроля серверов, баз данных, деятельности администраторов ЛВС в той или иной мере реализуются во многих программных продуктах, о двух из которых было вкратце рассказано.

Из всего вышесказанного можно сделать два основных вывода. Первый: с ростом количества компьютерной техники, используемой в кредитно-финансовых учреждениях, резко возрастает опасность злоупотреблений со стороны обслуживающих её специалистов. Второй: предотвращение подобных случаев должно быть поручено квалифицированным специалистам, вооружённым специальными программными продуктами.

Таким образом, при обеспечении безопасности банковских компьютерных сетей необходимо предусматривать не только меры по их защите от несанкционированного доступа внешнего злоумышленника, но и от злонамеренных действий легально зарегистрированных в системе пользователей, особенно обладающих правами администраторов.

А.А. Кабанов, канд. юрид. наук, доцент

Информационная природа открытий

Маленький ребёнок, впервые увидевший, как прыгает лягушка, совершает для себя открытие. Это открытие приносит ему радость. Юноша, впервые целующий девушку, также обнаруживает внутри себя настолько новые чувства, что воспринимает их как открытие. Даже старый и умудрённый опытом человек, осознающий вдруг, что, несмотря на ожидающее его небытие, жизнь всё-таки прекрасна и удивительна, также совершает для себя очередное открытие. Жизнь бесконечна в своём разнообразии. Как бы много ни узнал человек, количество неизвестной для него информации бесконечно больше. Умение удивляться, радоваться своим открытиям, — это замечательное человеческое свойство. Оно присуще всем людям, а, возможно, и не только людям.

В процессе познания мира человек улучшает свою жизнь, а также жизнь тех, кто его окружает. Он создаёт искусственную природу, вносит в неё дополнительное разнообразие. Это не только технические изделия вроде каменного топора, автомобиля, очков или компьютера. Это также комнатные растения, домашние животные, общение между людьми и многое другое, в том числе то, что трудно описать и даже понять. То есть, иногда человек создаёт то, что сам не в состоянии объяснить.

Во всём этом присутствует информация — степень снятия неопределённости, степень упорядоченности, сведения и сообщения.

Способы приобретения информации человеком различны. Иногда человек понимает, откуда он получил информацию. Но чаще информация появляется как бы ниоткуда. Тогда даже такой умный человек, как Иммануил Кант, в своих «Прологоменах» и в «Критике чистого разума» заявляет, что человек имеет априорную информацию. В частности, о пространстве и времени, о способах познания и многом другом. На самом деле, если спросить новорожденного, что такое пространство или время, вряд ли вы услышите вразумительный ответ. Прежде чем понять такие высокие абстракции, человек должен освоить опытную информацию о том, что такое горячо и что такое холодно, что такое сытно и что такое голодно, что дыхание возможно там, где есть воздух, и что только рыба может дышать водой, а также многое другое.

Каждая частичка новой информации, усвоенной человеком, является для него открытием. Многие открытия человек делает, даже не осознавая этого. Так называемую доопытную (априорную) информацию, умение предвидеть и упредить событие, Амосов называл антиципацией. Когда один из драчунов сознательно наносит другому удар, часто защита от удара выполняется гораздо быстрее и неосознанно. Некоторые люди заранее знают, что погода скоро изменится, и с большим трудом и притом не всегда могут потом объяснить, почему они в состоянии предвидеть будущее. Дело в том, что получаемая человеком информация далеко не всегда осознаётся. Часто она воспринимается неосознанно, а может быть «синтезируется» как будто бы новое знание после анализа каких-то фактов, событий или явлений. В тех случаях, когда вывод получается неожиданным, человек ощущает его как открытие.

Научным открытием принято называть такое, которое неожиданно не только или не столько для самого человека, сколько для других людей, которые, в свою очередь, и признают приоритет на него у этого первооткрывателя. Такому первооткрывателю вручают «Нобелевскую премию», или «Диплом на открытие» или ещё что-нибудь, но это не важно по сравнению с радостью самого открытия. И всё-таки, какова же природа открытия? Она материальна, а может быть заключается в какой-то энергии, в движении? В мире ведь нет ничего кроме движущейся материи.

Да нет, пожалуй, природа открытия – чисто информационная. И именно неожиданность получения новой информации, то есть снятие большой неопределённости воспринимается как открытие. Наверное, можно приблизительно оценить открытие как информацию, вероятность правильности которой оценивалась чрезвычайно низко, ну, к примеру, долями процента, но оказавшейся совершенно верной, при-

чём не интуитивно верной, как астрологический прогноз, а повторяющейся и проверяемой, как научный эксперимент. Открытие может быть получено в результате «случайного» озарения, в результате кропотливого сбора и анализа огромного количества малоценной на первый взгляд информации, или в результате и того и другого, то есть, как чаще всего и бывает, озарение наступает именно на основании обработки информации.

По мнению наиболее авторитетного компаративиста – Рене Да-вида, право – это модель общества. Причём не только вербальная модель, но и невербальная – в частности обычаи и обыкновения. Очевидно, что право – чрезвычайно сложная модель, позволяющая, однако, делать выводы, прогнозировать социальные явления и процессы. Существующие попытки моделирования социальных процессов чрезвычайно просты по сравнению со всей совокупностью права как явления. Попытки автоматизации правовых процессов, создание автоматизированных правовых информационных систем пока ещё не достаточно сложны. А ведь известен закон Акоффа о том, что система должна обладать достаточным разнообразием. Модель общества, претендующая на возможность совершать социальные открытия, также должна обладать таким разнообразием. Только тогда от такой модели будет реальная польза.

Известны попытки моделирования системы законодательства – информационно-справочные правовые системы. Многие из них построены по гипертекстовой структуре. Но нужны информационно-советующие системы. Нужны гипермедиа структуры социальных моделей. Современные технические устройства – компьютеры, их локальные и глобальные сети, в принципе позволяют сделать очередной крупный шаг в моделировании социальных процессов, сделать новое открытие. Очень может быть, что такое открытие помогло бы решить животрепещущие глобальные проблемы современности: проблемы терроризма, наркомании, демографические и экологические, да и многие другие. Ясно, что такое открытие тоже будет иметь информационную природу, как и многие другие открытия.

*Кабанов А.А, канд. юрид наук, доцент;
Кутузов О.В.;
Бугель Н.В., д-р юрид. наук, профессор*

Информационно–обучающие программы с использованием интернет технологий

В настоящее время существует много обучающих программ и справочно-информационных систем, используемых в учебном процессе. Примером их являются «Консультант+», «Кодекс», «Гарант» и др. Их применение позволяет значительно повысить эффективность и качество обучения слушателей и курсантов вузов МВД.

Вместе с тем, создание, обновление и использование приведённых выше программ не всегда обеспечивает решение поставленных учебных задач, т.к. различные программы не всегда обладают гибкой конфигурацией, написаны на различных языках программирования, а на обновление баз данных и конфигурации требуются постоянные материальные затраты.

Авторами предлагается создание информационно-обучающей программы для подготовки сотрудников ГИБДД с применением интернет технологий. В основу такой программы заложен широко применяемый язык программирования HTML. При создании базы данных использована бесплатная информация с автомобильных сайтов:

<http://autoworld.agava.ru>

<http://carsfoto.vov.ru>

<http://www.autoreview.ru>

Данная информация может предоставляться пользователям в двух форматах: а) для изучения внешнего вида и технических характеристик автомобилей различных марок; б) для самотестирования по избранной тематике.

В первом формате реализованы функции просмотра, аналогичные моделям веб-страниц с информационной базой данных автомобилей всех марок и моделей.

Сотрудник ДПС может тренировать себя запоминанию моделей автомобилей посредством просмотра базы. Просмотр возможен в режиме слайд-шоу, т.е. поочерёдной сменой фотографий и комментариев к ним. Также возможна сортировка по маркам, характеристикам, типам кузовов и т.д. В существующей базе данных представлен ряд из 1500 марок и моделей автомобилей с указанием их технических характеристик (Рис. 1).

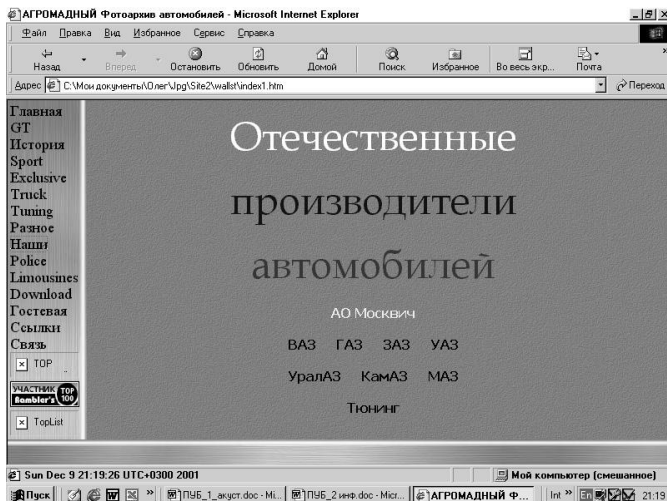
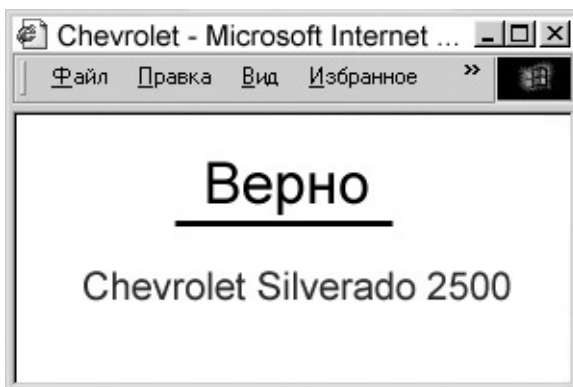


Рис.1 Общий вид базы

Во втором формате информация представляется в виде тестовой программы, написанной на языке программирования Java. Она позволяет в интерактивном режиме проводить самоконтроль знаний приобретённых при работе с базой (Рис. 1). После запуска программы на экране появляется фотография автомобиля, и три варианта ответа с названием марки и модели. Два из них неверны. В процессе теста набирается статистика, и в конце выводится результат с количеством верных/неверных ответов и процентом распознавания. Окно программы изображено на Рис.2.



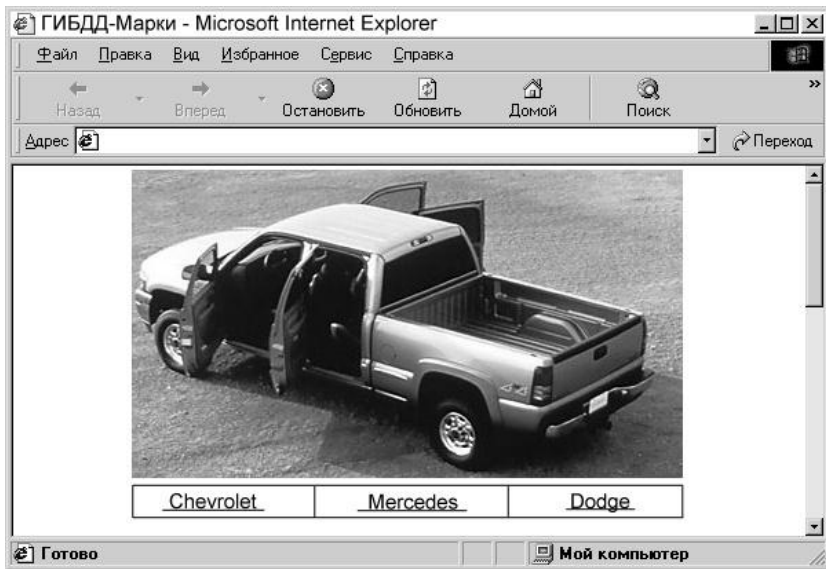


Рис.2 Общий вид программы самотестирования

Предложенные информационно-обучающие программы позволят повысить эффективность обучения сотрудников ГИБДД. Вместе с тем можно отметить следующее. Алгоритм построения таких программ можно применять и при решении других задач обучения.

*Калис Е.Б.;
Яковлев А.Ю.*

Объект и предмет неправомерного доступа к компьютерной информации

Компьютерные преступления впервые попали в сферу социального контроля в начале 1970-ых годов, когда в США было выявлено значительное количество преступлений, связанных с неправомерным доступом к компьютерной информации, совершённых в 1950–1970-е годы, не смотря на то, что первое преступления было зарегистрировано в 1966 г.

Данный феномен привлёк к сфере компьютерной информации большое внимание со стороны исследовательских институтов на наци-

ональном и международном уровнях. Стали формироваться специальные нормы о компьютерных преступлениях в уголовном законодательстве.

Неправомерный доступ к компьютерной информации представляет собой одно из самых малоизученных преступлений последнего времени, приобретающее всё более угрожающие масштабы. Его последствия таят реальную угрозу причинения вреда отношениям безопасности личности, общества и государства. Неправомерный доступ к компьютерной информации является наиболее распространённым видом общественно опасных деяний, рассматриваемых в главе 28 Особенной части Уголовного кодекса. По данным ГИЦ МВД РФ в 1997 году их удельный вес в общем числе зарегистрированных преступлений в сфере компьютерной информации составил 64 %.

Сегодня применение статьи 272 УК РФ сопровождается определёнными трудностями. Во-первых, отсутствием достаточной теоретической базы, судебной и следственной практики, а также официальных разъяснений Верховного суда и Генеральной прокуратуры РФ. Во-вторых, многие признаки данного состава преступления носят явно технический характер, что предполагает наличие знаний в области компьютерной техники. В то же время подготовка следователей, дознавателей и оперативных работников остаётся достаточно низкой. Всё это может повлечь неоднозначное применение норм уголовного закона и, следовательно, нарушение основополагающих принципов уголовного права – справедливости и законности. Точный анализ объекта и предмета указанного состава преступления, может устранить ошибки при квалификации деяния.

Разумеется, в борьбе с неправомерным доступом к компьютерной информации нельзя игнорировать организационные, технические и программные меры. Между тем, эффективное решение задачи по обеспечению законных прав и интересов личности, общества и государства в области информационной безопасности невозможно без адекватных мер уголовно-правового характера.

Юридическая квалификация любого преступления состоит в установлении тождества конкретных обстоятельств, противоправных деяний признакам конкретного состава преступления. Таким образом, квалификация преступления начинается с анализа объекта и предмета преступного посягательства.

Родовым объектом неправомерного доступа к охраняемой законом компьютерной информации является совокупность общественных отношений, обеспечивающих общественную безопасность и общественный порядок. Под безопасностью понимается состояние защи-

щённости, а повсеместная компьютеризация оборонных систем, спутников, атомных станций, создание компьютеризированных банков данных при их уничтожении, блокировании, модификации либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети может привести к катастрофическим последствиям. Это является одной из причин того, что данное преступление считается посягательством на безопасность общества.

Видовым объектом данного посягательства являются общественные отношения в части правомерного и безопасного использования компьютерной информации и информационных ресурсов. Выявление данного обстоятельства важно для того, чтобы отграничить неправомерный доступ к компьютерной информации от других преступлений УК РФ в тех случаях, когда компьютерная аппаратура является предметом преступления против собственности, а также когда происходит уничтожение элемента ЭВМ. Например, если виновный умышленно сжигает микропроцессор или выводит из рабочего состояния монитор, то его действия подлежат квалификации по соответствующей части ст. 167 УК РФ.

Непосредственным объектом являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети. Дополнительный объект факультативен, но его наличие повышает степень общественной опасности неправомерного доступа к компьютерной информации. Объект преступного посягательства – необходимый элемент любого общественно опасного и противоправного деяния. Безобъектных преступлений не может быть, так как в противном случае отсутствует сам факт преступного посягательства на охраняемые общественные отношения. В соответствии со статьей 5 УПК РСФСР указанное обстоятельство рассматривается как исключяющее производство по уголовному делу и, следовательно, оно подлежит немедленному прекращению.

Предмет неправомерного доступа к компьютерной информации является определяющим моментом в отграничении рассматриваемого состава от иных составов преступлений.

В диспозиции уголовно-правовых норм нередко содержится прямое указание на предмет преступного посягательства и его особенность. В ст. 272 УК РФ сказано об ответственности за неправомерный доступ к компьютерной информации. Поэтому есть все основания остановиться на особенностях предмета данного преступления, которые характеризуются следующими обязательными показателями:

1) компьютерная информация, как предмет преступления, предусмотренного ст. 272 УК РФ, всегда является интеллектуальной собственностью;

2) указанная информация – есть предмет, не обладающий натуральными физическими свойствами;

3) компьютерная информация охраняется законом;

4) информация содержится на машинном носителе в ЭВМ, системе ЭВМ или их сети.

Чтобы признать лицо виновным в совершении преступления, предусмотренного ст. 272 УК РФ необходимо установить, является ли компьютерная информация интеллектуальной собственностью. Воздействие на компьютерную информацию, не являющуюся предметом интеллектуальной собственности государства, юридического лица, группы физических лиц или отдельного физического лица, не образует признаков состава преступления, и, следовательно, нет оснований для привлечения к уголовной ответственности за подобное деяние. В диспозиции статьи в качестве предмета посягательства указывается не на электронно-вычислительную технику, а на компьютерную информацию (которая передается, обрабатывается и хранится с использованием электронно-вычислительной техники), что свидетельствует о её нематериальном характере.

Следующей специфической особенностью предмета преступления выступает компьютерная информация, охраняемая законом (конфиденциальные сведения о персональных данных, сведения, составляющие служебную, коммерческую, банковскую или государственную тайну), информация являющаяся объектом авторского права. Неправомерный доступ к компьютерной информации общего пользования, то есть к информации, адресованной неограниченно широкому кругу лиц, не образует признаков преступления, ответственность за совершение которого предусмотрена ст. 272 УК РФ.

Установление этого показателя позволяет не только с предельной точностью применить норму статьи закона к лицу, совершившему преступление, но и способствует отграничению неправомерного доступа к компьютерной информации от создания, использования и распространения вредоносных программ для ЭВМ (ст. 273 УК РФ), где предметом посягательства может выступать информация общего пользования, т. е. компьютерная информация, не охраняемая законом.

Необходимо отметить, что компьютерная информация, на которую воздействует преступник, содержится на машинном носителе, в системе ЭВМ или их сети. Рукописная информация, содержащаяся на бумаге или ином физическом носителе, не указанном диспозиции ста-

тии закона, не подпадает под понятие предмета преступления, предусмотренного ст. 272 УК РФ.

Существует тесная связь между предметом посягательства и объектом преступления, так как предмет является его частью и лишь формой, условием существования общественных отношений. Правильное определение объекта и предмета состава преступления обеспечивает точное отграничение неправомерного доступа к компьютерной информации от смежных составов, что влечёт за собой правильное применение закона (соблюдение принципов законности, гуманизма и принципа справедливости отправления наказания).

Правильное определение объекта и предмета преступления является хотя и необходимым, но всего лишь первоначальным этапом в идентификации преступного посягательства. Для окончательной квалификации необходимо нахождение, сопоставление и установление тождества всех элементов противоправного общественно опасного деяния и признаков состава преступления.

Киртаев А.С.

Защита информации в ходе предупреждения валютных правонарушений

В Законе РФ «О валютном регулировании и валютном контроле» 1992 года, основном российском нормативном акте в валютной сфере, для отнесения тех или иных действий к валютным операциям используется формальный метод. В п. 7 ст. 1 Закона даётся перечень юридических и фактических действий, образующих валютные операции.

Можно согласиться с точкой зрения И.В. Хоменушко, что валютные операции – «это предусмотренные валютным законодательством действия экономических субъектов, совершаемые в отношении валюты и валютных ценностей и подлежащие государственному регулированию и контролю для целей защиты национальной валюты»¹.

Экономическими субъектами являются резиденты и нерезиденты, которые обязаны совершать указанные действия строго в соответствии с гражданским и валютным законодательством Российской Федерации, содержащим определённые ограничения.

¹ Хоменушко И.В. Валютный контроль в Российской Федерации. Учебно-практ. пособие. – М.: ИД ФБК – ПРЕСС, 2001. – С. 32.

Поскольку нормы, адресованные участникам валютных отношений, представляют собой определённые ограничения на проведение операций с валютой (валютные ограничения), то необходим соответствующий валютный контроль, круг задач и направления которого зависят от круга валютных ограничений.

Субъектами валютного контроля являются органы и агенты валютного контроля. По смыслу ст. 11 Закона о валютном регулировании, органы валютного контроля – это органы государственного управления, наделённые компетенцией в сфере валютного контроля. В числе органов государственного управления, наделённых соответствующей компетенцией, Законом указаны Центральный банк Российской Федерации и Правительство Российской Федерации. Агентами валютного контроля являются «организации, которые в соответствии с законодательными актами Российской Федерации могут осуществлять функции валютного контроля», т.е. это уполномоченные банки, которые имеют лицензию Банка России на совершение банковских операций с иностранной валютой.

Однако необходимо констатировать, что на сегодняшний день круг органов и агентов валютного контроля значительно расширен. Так, в настоящее время к числу органов валютного контроля относится Государственный таможенный комитет Российской Федерации, что подтверждается прямым указанием ст. 198 Таможенного кодекса Российской Федерации.

Круг агентов валютного контроля расширился за счёт наделения соответствующими функциями государственных органов, таких как налоговые органы и ФСНП России, что определено Законом РФ «О налоговых органах Российской Федерации»¹. Однако всей полнотой прав органов валютного контроля они не наделены.

Субъектами валютного контроля в ходе осуществления своей деятельности используются установленные законодательством методы. Основными методами, используемыми субъектами валютного контроля, выступают наблюдение и проверка.

В ходе применения субъектами валютного контроля конкретных действий и процедур, остро встает вопрос защиты информации о деятельности хозяйствующих субъектов, совершающих валютные опера-

¹ См.: Федеральный закон от 8 июля 1999 г. № 151-ФЗ «О внесении изменений и дополнений в Закон РСФСР «О государственной налоговой службе РСФСР» // Собрание законодательства Российской Федерации. – 1999. – № 28. – Ст. 3484.

ции, которая становится известной органам и агентам валютного контроля. В данной области существуют некоторые проблемы.

Так, основными особенностями, которые присущи методу наблюдения, используемому органами и агентами валютного контроля, являются постоянность и всеобщность проводимого наблюдения.

Содержание такой особенности как всеобщность наблюдения заключается в том, что абсолютно все лица, которые совершают валютные операции, подлежащие наблюдению в силу указания законодательства, становятся объектами наблюдения органов и агентов валютного контроля. Наличие факта проведения валютной операции является поводом для осуществления субъектами валютного контроля процедуры наблюдения над проводимой лицом, то есть объектом наблюдения, операцией.

Однако согласно ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Поэтому всеобщее наблюдение, представляющее собой, в частности, создание электронных баз данных, за валютными операциями вошло бы в противоречие с конституционными правами и свободами граждан.

Принятые только в настоящее время правила это ограничение соблюдают. Так, Инструкция Банка России от 28 июня 1999 г. № 83-И, обязывающая уполномоченные банки создавать электронные базы данных о валютных операциях клиентов с последующей передачей информации в распоряжение органов валютного контроля, распространяет эту процедуру только на операции юридических лиц, являющихся клиентами этих банков.

На сегодняшний день значительной проблемой является предусмотренная той же инструкцией обязанность уполномоченных банков, как агентов валютного контроля, регулярно (ежедекадно) передавать всю информацию о валютных операциях своих клиентов – юридических лиц территориальным управлениям Банка России. В указанной выше Инструкции речь идёт о передаче сведений о договорах клиентов, однако, ясно, что реально происходит передача государственным органам информации о банковских валютных операциях, о расчётах по внешнеторговым контрактам. Между тем, согласно ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»¹ сведения об операциях клиентов представляют собой банковскую тайну. Справки по операциям юридических лиц могут выда-

¹ Собрание законодательства Российской Федерации. – 1996. - № 6. – Ст. 492.

ваться судебным органам, Счётной палате российской Федерации, налоговым органам, налоговой полиции, таможенным органам, а также органам предварительного следствия (с согласия прокурора). Территориальные управления Банка России, а также и сам Банк России, как органы валютного контроля, не названы Законом о банках и банковской деятельности в числе органов, имеющих доступ к банковской тайне. Тем самым Инструкция Банка России № 83-И вынуждает уполномоченные банки регулярно нарушать законодательство о банковской тайне.

Учитывая выше изложенное, ясно, что объектам валютного контроля остаётся уповать только на установленную в Законе РФ «О валютном регулировании и валютном контроле» и других нормативно-правовых актах РФ обязанность органов и агентов валютного контроля и их должностных лиц сохранять ставшую им известной при выполнении функций валютного контроля коммерческую тайну резидентов и нерезидентов.

Представляется, что допустимые пределы наблюдения в этом случае завышены и подлежат законодательному ограничению в дальнейшем. Однако сложившаяся на сегодняшний день ситуация в валютной сфере не позволяет утверждать, что пределы наблюдения органов и агентов валютного контроля за лицами, осуществляющими валютные операции будут ограничены в ближайшем будущем.

Дело в том, что положение дел в сфере операций с валютными ценностями просто катастрофическое. В последнее время в стране наблюдается криминальная активность преступных структур в кредитно-финансовой сфере. Особо крупных масштабов достигли незаконные операции по вывозу из России валютных средств, «отмыванию» преступно нажитых капиталов, незаконный сбор и использование информации о конкурентах.

Согласно оценкам отечественных экспертов «с 1990 года из Российской Федерации вывезено порядка 30-60 млрд. долларов США, в настоящее время вывоз капитала продолжается и достигает 1-2 млрд. долларов США в месяц»¹. «По прогнозам экспертов США, ежегодно из России вывозится 16-17 миллиардов долларов США»².

¹ Егоров В.А. Криминалистические модели экономических преступлений в кредитно-финансовой сфере. - Саратов: СЮИ МВД России, 1999. - С. 46.

² Зиновьев А.В. Экономическая преступность в России: проблемы и перспективы. // Вестник Санкт-Петербургского университета МВД России. № 2(6), 2000. - С. 131.

Таким образом, в ближайшее время усиление контроля за лицами, осуществляющими валютные операции со стороны органов и агентств валютного контроля, будет продолжаться. Однако параллельно этому необходима своевременная корректировка законодательства в области валютного регулирования и контроля в целях недопущения появления таких противоречий в законодательстве, как было указано выше и распространения информации, получаемой органами и агентами валютного контроля.

Г. И. Кожевников, канд. техн. наук;

О. Ю. Енов

Обеспечение безопасности сетей, связанных с INTERNET

Бурное развитие сетевых технологий, наблюдаемое в последние годы, обусловило широкое внедрение крупных информационных систем, основанных на территориально-распределённых корпоративных сетях. В настоящее время такие сети всё более и более интегрируются с **Internet**. Подключение к **Internet**, кроме престижа, становится всё более необходимым. Это вызвано появлением многочисленных услуг, которые предоставляет **Internet**: глобальная электронная почта, практически всемирная реклама, оперативное получение информационных новостей, доступ к современным информационным и программным ресурсам, оперативное получение консультаций квалифицированных специалистов, возможность организации совместной работы территориально разнесённых групп, электронная торговля, удалённый доступ к ресурсам корпоративной сети, использование речевой и видеoinформации и т.п.

Эти и другие, предоставляемые **Internet**, услуги привели к применению различными корпоративными сетями Web- технологии (такие сети стали называться **intranet**). Основным препятствием, сдерживающим такого рода подключения, являются общеизвестные факты нарушения безопасности в **Internet** и через **Internet**. По данным Федерального бюро расследований США ежегодный ущерб от различных компьютерных преступлений составляет около 7,5 млрд. долларов. Согласно этим данным 80 % подобных преступлений совершается через **Internet**. Эти цифры являются заниженными, поскольку многие атаки не были обнаружены или потерпевшие не сообщили об имевших место атаках, чтобы не уронить своего престижа. Поэтому для **intranet** сетей проблемы безопасности выходят на первый план, поскольку, помимо

защиты информации в своей корпоративной сети, необходимо учитывать возможность атак со стороны **Internet**.

Проблема необходимости защиты информации привела к появлению целой отрасли индустрии - разработка и производство средств защиты данных. Из арсенала государственных, военных и специальных служб средства защиты стали достоянием различных пользователей. Но, несмотря на уже имеющийся громадный арсенал разнообразных средств защиты, процесс вторжения в компьютерные системы продолжается и до настоящего времени, причём число вторжений постоянно растёт.

В качестве основного средства защиты при подключении к **Internet** рекомендуются различные межсетевые экраны (**firewalls**). Сетевые экраны проводят анализ входящего и исходящего трафика и на основе заложенных в них правил безопасности принимают решение о разрешении или запрещении передачи данных. Контроль информационных потоков межсетевым экраном состоит в их фильтрации, то есть выборочном пропуске пакетов через экран. Фильтрация осуществляется на основе набора правил, который загружается на этапе инициализации и представляет собой формальное представление аспектов политики безопасности корпоративной сети. Существует большое количество разнообразных межсетевых экранов. Их обычно классифицируют по уровню, на котором производится фильтрация (канальный, сетевой, транспортный, прикладной и смешанный).

В настоящее время на рынке существует множество различных экранов, решающих те или иные вопросы защиты. Сложные экраны осуществляют фильтрацию различных протоколов с помощью настраиваемых администратором фильтров. Фильтрация может осуществляться на уровне кадров, пакетов, каналов и приложений. Кроме того, экраны обычно содержат различные средства аудита происходящих событий, что позволяет администратору проводить анализ данных для оценки качества защиты. Хотя такие экраны и представляют собой мощные средства обеспечения безопасности, но в то же время они не могут обеспечить стопроцентную защиту. Кроме того, обычно большинство случаев проникновения через сетевые экраны связаны с неправильным или ошибочным администрированием экранов. Это объясняется сложностью администрирования экрана и отсутствием экранов, контролирующих все известные пути проведения, атак. Поэтому наличие только одного сетевого экрана не решает проблем безопасности.

Поскольку существует множество экранов с различными реализованными функциями фильтрации (не все межсетевые экраны обла-

дают функциональной полнотой), появляется необходимость унифицированного средства, устраняющего недостатки экранов и облегчающего процессы конфигурирования, - сетевого процессора безопасности. Такой сетевой процессор предназначен для обеспечения следующих функций защиты:

- фильтрация трафика по адресам и портам источника и приёмника, а также на прикладном уровне (функции межсетевого экрана);

- сжатие данных перед шифрованием;

- обеспечение конфиденциальности и целостности информации за счёт шифрации IP-пакетов и организации виртуальных защищённых каналов в сетях общего пользования;

- расширенный аудит с выводом результатов из журналов наблюдения на рабочее место администратора безопасности;

- обеспечение мониторинга безопасности и удалённого управления сетью.

Такой сетевой процессор безопасности предназначен для предотвращения утечки, хищения, несанкционированного уничтожения и модификации передаваемой по сети информации. Как и экран, процессор осуществляет защиту адресного пространства подключаемых локальных сетей.

Реализация основных функций защиты в сетевом процессоре безопасности позволяет достаточно легко вводить новые функции, связанные с защитой от новых типов атак. Применение шифрующего устройства отечественного производства позволяет использовать его для защиты сетей с критической информацией.

Г. И. Кожевников, канд. техн. наук;

Е.А. Сухогозова

Информационное обеспечение управленческой деятельности

Любой человеческий труд не представляется возможным без информационных процессов. Однако есть особые виды деятельности, где информация является одним из основных её элементов. Важное значение принадлежит информации в управленческой деятельности¹.

¹ В науке понятие «информация» впервые прозвучало в 1948 году в работе Клода Шеннона «Математическая теория связи». Закон единства управления и информации в организационных системах различной природы впервые

Здесь информация выступает и как *предмет труда* (например, статистические данные), и как *средство управляющих воздействий* (например, приказ), и как *средство обратной связи* (например, отчёт), и как *продукт труда* (например, аналитическая справка). Поэтому информационное обеспечение управленческой деятельности позволяет не только оперативно управлять силами и средствами, но и своевременно оказывать помощь подчинённым структурам, а также влиять на организацию и конечные результаты их работы.

Общепринятым является подразделение информации на несколько основных типов: *биологическую, техническую и социальную*. А, поскольку управленческая деятельность - это деятельность в сложных социальных системах, то главным типом информации будет являться *социальная информация*.

Используемая в управленческой деятельности социальная информация может быть классифицирована по самым различным основаниям (признакам). Так, информация, обеспечивающая деятельность системы, делится на *внешнюю*, поступающую из других организаций и ведомств, и *внутреннюю*, которая вырабатывается непосредственно в результате осуществления системой определённых социальных функций.

Существует и другой подход к классификации информации в управленческой деятельности, где выделяются следующие её виды:

- *директивная (организационно-исполнительная) информация*, определяющая и регулирующая деятельность системы, её основные задачи, функции, целевые установки и разовые задачи;
- *аналитическая информация*, содержащая анализ той или иной стороны деятельности системы, а также факторов и явлений, имеющих отношение к её деятельности¹;
- *прогнозная информация*, дающая прогностические оценки отдельных явлений, касающихся деятельности системы;
- *учётно-контрольная и отчётная информация*, характеризующая состояние и результаты функционирования системы и объектов внешней среды;
- *методическая информация*, определяющая или рекомендуемая те или иные способы наиболее эффективного функционирования

был сформулирован наукой кибернетикой и является одним из важнейших научных принципов.

¹ Такой анализ может относиться как к системе в целом, так и к отдельным составляющим её частям. Он охватывает, как правило, различные временные периоды (квартал, год и т.п.).

системы и организацию взаимодействия между отдельными её элементами;

- *справочная*, то есть информация, содержащая сведения справочного и вспомогательного характера, необходимые для организации деятельности системы;

- *оперативно-служебная*, содержащая текущую переписку с вышестоящими и смежными системными образованиями по определённым вопросам их деятельности, а также с объектами внутреннего управления.

Совокупность различных видов информации, объектов управления, их связь между собой образуют *систему информации*, которая в свою очередь также характеризуется рядом признаков:

1. Она должна охватывать *все* необходимые *виды информации*, находящие применение в конкретной области управления.

2. В ней должны осуществляться двухсторонние информационные связи (*прямая и обратная связь*). Субъект управления (начальник) как управляющий орган вырабатывает и направляет объектам управления (подчинённым) соответствующее управленческое решение. В свою очередь объекты управления должны предоставить управляющему органу информацию о ходе и результатах выполнения управленческого решения¹.

3. Наличие в ней определённой *организации информационных потоков*, связывающих как составные её элементы, так и систему управления с внешней средой.

Таким образом, процесс управления связан с непрерывным обменом информацией между субъектами управления, объектом управления и средой функционирования.

Не располагая сведениями об объекте и субъекте управления, а также об условиях, в которых они действуют, невозможно успешно управлять. Без поступления информации о состоянии объекта управления не может быть целенаправленного воздействия на него. В свою очередь никакие воздействия на объект управления не могут иметь место без поступления соответствующих команд управления.

¹ В организации информационно-аналитической работы и в управлении в целом обратные связи имеют особое значение, поскольку они способствуют не только уставной и исполнительной дисциплине, но и объективно указывают на обоснованность принятия тех или иных управленческих решений и на их эффективность.

Обобщая вышесказанное, можно утверждать, что система информационного обеспечения управленческой деятельности будет состоять в следующем:

сборе внутренней и внешней информации о состоянии окружающей её среды;

передаче этой информации по каналам связи к месту её переработки;

переработке информации с целью формирования управленческого решения;

передаче управленческого решения (на основе переработанной информации) исполнительным органам;

контроле за реализацией и исполнением управленческого решения.

Современное состояние развития науки наглядно показывает взаимосвязь методов исследования информации в сфере общественных отношений. Среди наиболее практикуемых общенаучных методов следует выделить **логические** методы, вытекающие из диалектической и формальной логики, **анализ, синтез, сравнение и выдвижение гипотез** и др.

В информационном обеспечении управленческой деятельности широко применяются теоретические и методологические положения, вырабатываемые социологией, кибернетикой, наукой управления, математикой, социальной психологией. Так, анализ и обработка социальной информации может производиться с учётом применения специальных познаний в области общей теории статистики: принципов группировки и распределения статистических величин, порядка определения средних и относительных показателей, приёмов преобразования показателей динамических рядов и т.д. Такие методы называются **статистическими**. Они позволяют, основываясь на диалектическом единстве необходимого и случайного, определять количественные параметры изучаемых социальных процессов и явлений.

Наряду с применением статистических методов при анализе социальных явлений всё шире используются **математические методы**, причём для изучения не только количественной стороны социальных процессов, но и их качественного своеобразия. Возможность применения этих методов объясняется тем, что массовые, устойчивые, повторяющиеся процессы имеют как *количественную*, так и *качественную* характеристики и эти характеристики находятся в единстве и взаимозависимости.

В комплексе методов научного исследования в настоящее время возрастает роль *математического моделирования*, что в определённой мере связано с развитием кибернетики.

Всё более широкое применение в информационном обеспечении находят *методы социальной психологии*.

Однако следует различать и методы отдельных направлений информационного обеспечения управленческой деятельности.

В информационном обеспечении управленческой деятельности наиболее распространены следующие *методы сбора и обработки информации*:

1. Наблюдение.
2. Опрос.
3. Изучение документов.
4. Эксперимент.

Другим важным направлением информационного обеспечения являются *методы накопления и систематизации информации* за определённый период времени. Например, накопление и систематизация сведений за сутки даёт возможность сформировать декадную, а затем месячную информацию.

Сбор и систематизация информации о деятельности системы и подчинённых структур осуществляется штабами, информационными центрами, отраслевыми службами.

Однако часто бывает невозможно принять управленческое решение без грамотного комплексного использования целого ряда приёмов, способов и средств сбора, систематизации, обобщения и анализа информации. Поэтому для решения конкретных задач управленческой деятельности необходимо создавать специальные методики, включающие в себе приёмы и способы исследования, присущие общенаучным и частнонаучным методам.

Методика вырабатывается на базе комплексной оценки информации, характеризующей состояние системы, условия и результаты её функционирования.

Специальные методики должны предусматривать следующие вопросы:

1. Круг и объём информации, необходимые для решения аналитических задач.
2. Способы сбора исходного материала.
3. Конкретные приёмы и методы анализа информации.

Все эти вопросы должны разрабатываться при выдвижении возможных гипотез о закономерностях изучаемых явлений, с учётом цели исследования. Целесообразно в связи с этим рассмотреть также неко-

торые приёмы и способы методов исследования информации в управленческой деятельности.

Для улучшения информационного обеспечения управленческой деятельности рекомендуется создавать централизованные информационно-справочные фонды, где будут находиться копии нормативно-методических, информационно-аналитических и справочных документов, справок по результатам выезда на места для инспектирования и целевых проверок; материалов совещаний, планов работы и других управленческих документов. Здесь же можно создать фонд (сборники) статистических данных о населении и социально-экономическом развитии региона, различных социологических исследований, перспективных и текущих планов других учреждений и организаций.

Таким образом, информационное обеспечение управленческой деятельности представляет собой сложную задачу.

О.А. Кокорева, канд. юрид. наук

Государственное лицензирование в системе информационной безопасности

Констатация цели разрешительной системы – обеспечение безопасности граждан, общества и государства, оставляет открытым ряд вопросов, в частности, о роли и месте разрешительной системы в государственном механизме обеспечения информационной безопасности. Предпринятый теоретико-правовой экскурс в понятие, содержание и предмет сферы информационной безопасности, позволил конкретизировать специфику, роль и место разрешительной системы в её обеспечении.

Во-первых, разрешительная система, как и система информационной безопасности, неразрывно связана с социальной деятельностью людей, несущей угрозы жизненно важным интересам личности, общества и государства. Потенциальность угрозы может быть связана как с опасным характером самой деятельности, так и с отношением субъекта деятельности к порядку и процедурам её осуществления. Поэтому разрешительная система как правовой инструмент обеспечения информационной безопасности в качестве обязательного элемента включает в себя наличие относительного запрета, а для его преодоления необходимо специальное разрешение, наличие которого порождает специфический вид общественных правовых отношений – разрешительных правоотношений.

Во-вторых, информационная безопасность охватывает практически *все* стороны жизнедеятельности людей. Разрешительная же система ограничена только *определёнными видами деятельности*. Для системы информационной безопасности не может быть избыточным объём охватываемых факторов, обстоятельств, условий, направлений деятельности, поскольку, чем он полнее, тем эффективнее обеспечивается информационная безопасность личности, общества, государства. Разрешительная система, сочетая частный и публичный интерес, не должна применяться в большем объёме, чем это необходимо для нейтрализации потенциальных опасностей *отдельных видов деятельности*. Избыточность разрешительных правоотношений создаёт напряжённость в отношениях между властными и невластными их субъектами, открывая путь для бюрократизма, волокиты, коррупции.

В-третьих, национальная безопасность является *государственно-правовой категорией*, все её составляющие в той или иной степени зафиксированы в Конституции Российской Федерации, которая в силу своего правового статуса институализирует жизненно важные интересы личности, общества, государства. Разрешительная система – *административно-правовая категория*, определённый правовой режим, непосредственно связанный с обеспечением охраны общественного порядка и безопасности на основе установления и реализации совокупности правил осуществления строго ограниченных законодательством видов социальной деятельности.

Центральным звеном разрешительной системы, правовым инструментом её осуществления является *лицензирование*, представляющее собой специфический административно-правовой метод государственно-управленческой деятельности и государственного регулирования. Понятие «лицензирование» как разновидность разрешительной политики государства относительно недавно введено в обиход отечественной административно-правовой науки, поэтому пока нет устоявшихся теоретических представлений о его правовой сущности, взаимосвязи с иными методами административно-правового регулирования, выполняемых функций.

Анализ законодательных и подзаконных правовых актов, регламентирующих лицензионные отношения, приводит к выводу о том, что по своей административно-правовой природе лицензирование относится к категории *нормативных методов регулирования*. Оно включает *полномочного субъекта* исполнительной власти – лицензирующие органы, действующие в определённой для них законодательством сфере деятельности. Лицензирование относится к категории *правонадельных* регулятивных методов управления, поскольку наделяет ли-

цензиата – юридическое лицо или индивидуального предпринимателя – правом на осуществление конкретных видов деятельности, ведение которых без соответствующей лицензии (разрешения) является незаконным и влечёт за собой предусмотренную действующим законодательством юридическую ответственность. Лицензирование является *административно-правовым методом*, органически сочетающим в себе *прямое* (например, директивная регламентация *процедур* получения лицензии, сроков её действия, оснований для приостановления или аннулирования) и *косвенное* властное административное воздействие, находящее своё отражение в своеобразных формулах: «делай, как приказано» и «делай, как лучше».

Лицензирование как специфический административно-правовой метод реализации полномочий исполнительных органов, органически сочетает в себе две функции – *охранительные* и *регулятивные*. Охранительная функция лицензирования связана с тем, оно распространяет своё действие на такие виды социально значимой деятельности, осуществление которых без соблюдения определённых требований и условий может повлечь за собой нанесение ущерба правам, законным интересам, нравственности и здоровью граждан, обороне страны и безопасности государства.¹ Регулятивная функция лицензирования связана с регулированием порядка производства определённых видов товаров и услуг путём *упорядочения функционирования* индивидуальных предпринимателей, государственных и негосударственных организаций, учреждений в целях сбалансированного осуществления ими социально значимых видов деятельности, установления правовых основ единого рынка.

Для лицензионных отношений характерно сочетание *публично-правовых* и *частно-правовых интересов*. Учитывая характер видов деятельности, подлежащих лицензированию, оно в первую очередь связано с обеспечением публичных интересов, лежащих в сфере обеспечения информационной безопасности личности, общества, государства. Выдвижение в этой триаде на первое место безопасности личности не только не уменьшает степень публично-правового, но и ещё раз подчёркивает *государственно-правовой характер* обеспечения этого вида безопасности, вытекающий из ст. 2 Конституции России, провозгласившей, что признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Реализуя эту обязанность, государство и устанавливает определённые правила осуществления тех видов деятельности, которые могут нанести ущерб правам и

¹ СЗ РФ. 1998. № 9. Ст. 4857.

законным интересам граждан, их здоровью – физическому и духовно-му. *Установление таких правил, контроль и надзор за их неукоснительным соблюдением относится к сфере действия административно-правовых норм.*

Частно-правовые интересы, реализуемые в лицензионных отношениях, лежат в сфере действия *гражданско-правовых норм*: во-первых, лишь с получением лицензии на осуществление тех видов деятельности, которые подлежат лицензированию, у юридических лиц возникает полная правоспособность, включая право на осуществление такой деятельности (ст. 49 ГК РФ); во-вторых, лицензия может выступать как составной элемент прав и обязанностей участников гражданско-правовых отношений (п.3 ст. 559, п. 2 ст. 656, п. 1 ст. 1031 ГК РФ); в-третьих, выдача лицензии предполагает государственное удостоверение того *юридического факта*, что лицензиат может осуществлять разрешённую ему деятельность в соответствии с *государственными стандартами безопасности*: техногенной, экологической, продовольственной, социальной и т.д., в силу чего лицензию можно рассматривать как определённую *гарантию* качественного выполнения лицензиатом договорных обязательств, зафиксированных в договоре или принятых на себя по умолчанию (например, ст. 789 ГК РФ), а нарушение лицензионных условий, повлекшее за собой наступление вреда, может рассматриваться как *юридическое основание наступления гражданско-правовой ответственности* (ст. 1079 ГК РФ).

Отмеченные обстоятельства не превращают лицензирование в гражданско-правовой институт или метод осуществления гражданско-правовых отношений, свидетельствуя лишь о том, что правовое регулирование лицензионной деятельности *должно учитывать гражданско-правовые последствия* её осуществления, предусматривая, например, в качестве *правового условия выдачи лицензии* обязательное имущественное или личное страхование соответствующих рисков.

Общность юридической природы лицензионных и административно-правовых отношений не означает их полную тождественность. Например, не все субъекты административно-правовых отношений могут быть субъектами лицензионных отношений, в большинстве случаев их возникновению, изменению или прекращению предшествует деятельность специальных структур – экспертных советов, комиссий, действующих как при лицензионном органе, так и независимо от него.

Особенности лицензионных отношений не могут служить основанием для сомнений в их административно-правовой природе. Происходит естественный процесс становления нового административно-правового метода государственного регулирования. Его общность с

иными аналогичными методами деятельности исполнительной власти не означает тождества в частных вопросах. Нельзя забывать и о процессах взаимопроникновения различных методов правового регулирования общественных явлений. Административно-правовые отношения не существуют изолировано от иных общественных отношений, регулируемых нормами права, а поэтому, не могут рассматриваться и существовать вне общего механизма правового регулирования, не испытывая на себе влияние иных отраслей и институтов права и не оказывая на них обратного влияния.

В этой связи особое значение приобретают вопросы полноты и качества *административно-правового регулирования* лицензионных отношений. По нашему мнению, принятие Федерального закона «О лицензировании отдельных видов деятельности» стало заметным шагом вперед на пути правовой упорядоченности лицензионных отношений. Однако общее состояние этого регулирования, а также юридическое качество самого закона вызывает немало вопросов.

Обращаясь к анализу инструментально-правовых и технико-юридических свойств этого закона с точки зрения полноты, точности и непротиворечивости операционализации правовых свойств лицензионных отношений, можно сделать следующие выводы. Во-первых, законодатель необоснованно отказался от распространения действия закона на все виды деятельности, подлежащие лицензированию по смыслу ст. 1, изъяв из юрисдикции закона внешнеторговую и таможенную деятельность, деятельность по охране окружающей среды, деятельность, связанную с использованием природных ресурсов, а также отношения, возникающие в связи с использованием результатов интеллектуальной деятельности, хотя все перечисленные виды деятельности имеют непосредственное отношение к обеспечению национальной безопасности, включая такие её виды, как безопасность экономическая, экологическая и социальная.

Во-вторых, законодатель фактически закрепил множественность законодательных актов, действующих в сфере лицензирования, отказавшись от их кодификации в рамках единого законодательного акта. В результате на сегодняшний день вопросы лицензирования разных видов деятельности регулируются несколькими десятками федеральных законов, что противоречит декларируемой в ст. 1 цели обеспечения *единой государственной политики* при осуществлении лицензирования, порождает многочисленные правовые коллизии и конкуренцию правовых норм, затрудняет ознакомление заинтересованных должностных лиц и граждан с полным перечнем подлежащих лицензированию видов деятельности.

В-третьих, существенным пробелом закона является отсутствие в нём упоминания об ответственности лицензионных органов за неправомерный отказ в выдаче лицензии, незаконную выдачу лицензии либо уклонение от выдачи лицензии.

В-четвертых, недостатком закона является и то, что в нём нет чёткого определения предметов ведения федерального центра и субъектов федерации и правовых основания распределения полномочий между ними в сфере лицензирования.

Таким образом, декларированные в законе цели лицензирования – обеспечение единой государственной политики, требует дальнейшего совершенствования правового регулирования в этой сфере. Поддерживая идею о разработке единого федерального реестра лицензированных видов деятельности мы, в свою очередь, полагаем целесообразным разработку лицензионного Кодекса РФ.

А.В. Костюк, канд. техн. наук, доцент

Применение новых информационных технологий в учебно-воспитательном процессе

Важнейшая роль в развитии современного общества в последней четверти XX – начале XXI века, бесспорно, принадлежит информатизации. Под информатизацией общества понимается всеобщий социальный процесс производства и повсеместного использования информации как общественного ресурса, обеспечивающего интенсификацию экономики, ускорение научно-технического прогресса и процесса интеллектуализации общества.

Информатизация общества предусматривает массовое внедрение методов и средств сбора, обработки, передачи и хранения информации на базе средств вычислительной техники (ВТ) и средств передачи информации.

В процессе информатизации общества логично выделить пять основных направлений:

- 1) комплексная автоматизация средств труда, технологических и производственных процессов;
- 2) информатизация научных исследований, проектных работ и технологической подготовки производства;
- 3) информатизация организационно-экономического управления;
- 4) информатизация сферы услуг и быта населения;

5) информатизация процессов обучения и подготовки кадров.

В информационном обществе центр тяжести в общественном разделении труда перемещается на производство, переработку и использование информации, резко возрастает наукоёмкость общественного производства, повышаются требования к уровню общекультурной и общенаучной подготовки всех участников общественного производства.

Требование общества о необходимости создания условий для непрерывного образования его членов неразрывно связано с развитием информатизации образования. Непрерывное образование и информатизация являются фактически двумя сторонами одного и того же процесса - повышения компетентности членов общества.

Информатизация образования невозможна без перехода в учебно-воспитательном процессе на новые информационные технологии (НИТ). НИТ в образовании есть комплекс учебных и учебно-методических материалов, технических и инструментальных средств вычислительной техники (СВТ) учебного назначения, а также система научных знаний о роли и месте СВТ в учебном процессе, о формах и методах их применения для совершенствования труда преподавателей и обучаемых.

Главная отличительная черта НИТ состоит в том, что они предоставляют практически неограниченные возможности для самостоятельной и совместной творческой деятельности преподавателей и обучаемых. Как показывает опыт, НИТ практически бесполезны при традиционном информационно-объяснительном подходе к обучению. В условиях НИТ меняется позиция педагога в учебном процессе. Из авторитетного носителя истины он превращается в соучастника продуктивной деятельности своих воспитанников. НИТ предполагает качественный сдвиг в отношениях между педагогами и обучаемыми.

НИТ становятся основной движущей силой развития. Во всех сферах образования и подготовки кадров ведутся поиски способов интенсификации и быстрой модернизации системы образования, повышения качества обучения путём применения компьютеров для поддержки самостоятельной познавательной деятельности обучаемых различных категорий, интенсификации труда преподавателей, управления работой учебных заведений.

Особую остроту приобретает вопрос непрерывной опережающей подготовки и переподготовки специалистов самых различных категорий к эффективному использованию НИТ, современных компьютеров в своей деятельности. Умение пользоваться вычислительной техникой при решении профессиональных и учебных задач приравни-

вается сейчас ко второй грамотности. От её уровня и распространения прямо зависят развитие научно-технического прогресса, интенсификация, модернизация и интеллектуализация производства и самой системы образования.

А.В. Костюк, канд. техн. наук, доцент;

Е.А. Макарова

Структура автоматизированной системы обучения и управления кафедры

Проведённый анализ возможностей персональных ЭВМ как средств обучения и управления учебной деятельностью показывает, что компьютер может выполнять как функции обучения, так и функции управления. С учётом возможностей компьютера и задач, решаемых на кафедре, может быть предложена следующая структура автоматизированной системы обучения и управления кафедры. Автоматизированная система - это человеко-машинная система коллективного пользования, работающая в диалоговом режиме и предназначенная для автоматизации процесса обучения, информационного обеспечения кафедры, а также моделирования обучающей среды с целью индивидуализации и интенсификации учебного процесса.

Основными элементами системы являются:

- 1) информационные и обучающие подсистемы;
- 2) пользователи АСОУК;
- 3) техническое обеспечение;
- 4) общесистемное обеспечение;
- 5) обслуживающий персонал.

Информационное и учебно-методическое обеспечение образуют следующие подсистемы:

руководящие документы;
 планирующие документы;
 программы и тематические планы учебных дисциплин;
 учебно-методические материалы;
 обучающие и информационные программы;
 успеваемость курсантов;
 кадры;
 командирская подготовка;
 учёт материальных средств;
 информационные данные.

Подсистема «руководящие документы» выполняет функции поиска и выдачи основных положений руководящих документов (прика-

зов и директив) по организации и ведению учебного процесса, работе с кадрами, организации службы войск, укрепления воинской дисциплины, организации эксплуатации и хранения вооружения и техники.

Подсистема «планирующие документы» состоит из разделов годового и месячного планов, плана повышения профессионального мастерства преподавателей, планов военно-научной, редакционно-издательской и рационализаторской работы и плана развития учебно-материальной базы кафедры. Подсистема обеспечивает реализацию информационных и управленческих функций.

Подсистемы «программы и тематические планы учебных дисциплин», «учебно-методические материалы» и «успеваемость курсантов» выполняют функции поиска информации в базах данных конкретной предметной области (информатика, вычислительная техника, математика и т.д.) дисциплины, раздела, темы.

Подсистема «обучающих и информационных программ» представляет собой совокупность сценариев учебных занятий, реализованных на персональной ЭВМ программными средствами, раскрывающих область знаний (умений) конкретной дисциплины (раздела, темы) и управляющих познавательной деятельностью обучаемых с целью достижения требуемых учебных целей (изучение и систематизация знаний, привитие и закрепление навыков в практической деятельности, контроль знаний, умений, навыков и т.п.). Подсистема обеспечивает выдачу в соответствии со сценарием занятия порции учебной информации (информационной, обучающей, контролирующей, справочной, расчётной, программируемой и т.п.) в виде произвольной последовательности (вопросов-эталонов, ответов и моделей - аналитических, графических, эвристических). Модели могут использоваться для иллюстрации процесса обучения, частичного управления процессом обучения, закрепления учебного материала и оценки качества знаний.

Подсистема «кадры» реализует информационную функцию. Она обеспечивает выдачу автобиографических данных личного состава кафедры, прохождение службы офицерами и прапорщиками, учебную, методическую и научную загрузку преподавателей, результаты проверок и успеваемости по командирской подготовке.

Подсистема «учёта» материальных средств обеспечивает учёт материальных средств по службам училища: по службе ракетно-артиллерийского вооружения, по учебному отделу, по квартирно-эксплуатационной и вещевой службам.

Подсистема «информационные данные» реализует поиск и выдачу справочных данных по общей тактике, тактике внутренних войск,

стрельбе и боевой работе, технической и огневой подготовке, дисциплинам гуманитарных и юридических кафедр.

Подсистема редактирования обеспечивает возможность оперативно заносить во внешнюю память учебную информацию с последующим редактированием, редактировать справочник информационно-поисковых подсистем, редактировать таблицы связей между разделами и эталонами, разделами и темами, а также редактировать общие связи между эталонами и моделями, поддерживающими процесс обучения.

Учебно-методическое обеспечение системы представляет собой совокупность учебного материала, методических указаний и статистических данных. Учебный материал, определённым образом отобранный и формализованный, включает в себя различные теоретические сведения, модели объектов и процессов изучаемой предметной области, наборы задач и проблемных ситуаций, описание алгоритмов решения учебных задач и т.п. И учебный материал, и методические указания являются, как правило, принадлежностью сценариев занятий и поэтому часто входят в обучающую программу.

Пользователи АСОУК делятся на три группы - авторы, преподаватели и обучаемые.

Авторы разрабатывают обучающие и информационные программы отбирают и формализуют учебный материал, составляют сценарии учебных занятий с учётом целей и методики обучения по конкретной дисциплине; реализуют их программными средствами, готовят необходимую документацию.

Преподаватели применяют обучающие программы при проведении учебных занятий осваивают обучающие программы (ОП); организуют работу обучаемых с ОП; при необходимости корректируют процесс взаимодействия обучаемых с ОП; анализируют статистические данные о работе обучаемых.

Обучаемые непосредственно используют обучающие программы в ходе учебного процесса (на занятиях, самоподготовке, тренировках т.п.).

Под техническим обеспечением понимается технический комплекс АСОУК, в состав которого входят персональные ЭВМ с их общим программным обеспечением, терминалы (дисплеи, устройства печати, графопостроители), средства комплексирования (создание сетей ЭВМ или локальных сетей) и сопряжения. На базе этих средств организуются классы персональных ЭВМ с необходимым количеством рабочих мест.

О. В. Кутузов

**К вопросу о применении современных компьютерных технологий
для морально-психологической подготовки оперативных
сотрудников органов внутренних дел**

Известно, что при выполнении служебных задач сотрудники органов внутренних дел в соответствии с нормативными документами имеют право применять огнестрельное оружие и специальные средства.

Однако проведённый анализ показывает, что эффективность их применения в боевой обстановке не всегда достаточна. Одним из факторов, отрицательно влияющих на качество подготовки оперативных сотрудников ОВД является то, что при проведении стрелковых тренировок и занятий по тактико-специальной подготовке не полностью обеспечиваются условия, приближающие их действия к реальной боевой обстановке. Вместе с тем известно, что сильные акустические воздействия (выстрелы, взрывы, шумы транспортных средств, крики людей и т.д.) отрицательно сказываются на морально психологическом состоянии человека и как следствие, приводят к снижению эффективности его действий в сложной обстановке.

Стоит отметить, что данные факторы частично учитываются при проведении стрелковых тренировок на специальных тренажёрах с использованием стереонаушников. Однако при этих условиях нельзя обеспечить выполнения практических упражнений в движении по причине связи наушников с тренажером механически (проводом), да и сами наушники не обеспечивают необходимого качества передачи акустических сигналов.

Для решения задачи улучшения качества морально-психологической подготовки сотрудников в ходе практических занятий, создания акустических эффектов и условий, приближённых к боевым, предлагается использовать современные цифровые технологии - аппаратно-программный комплекс типа Dolby Digital Рис.1.



Рис.1

В современных компьютерах типа IBM PC используются технологии «объёмного звука». Четырёхканальная схема (квадрофония) выглядит наиболее простой, упрощает коммутацию аппаратуры и размещение колонок – однако она требует применения наиболее высококачественных фронтальных динамиков. Дело в том, что в данной задаче очень важно адекватно и без искажений передать низкочастотные звуки большого уровня - на них лежит основная нагрузка создания «эффекта события» (взрывы, звуки самолета, вертолета, перестрелка) – а это требует большого запаса по мощности и способность акустики воспроизводить низшие звуковые частоты. Поэтому достаточно часто четырёхканальную схему превращают в пятиканальную, используя сабвуфер.

К сожалению, четырех- и пятиканальные схемы обладают ещё одним недостатком – эффект объёмного звука в них локализован в очень небольшой оптимальной зоне, что позволяет применять их в ос-

новном для индивидуальных тренировок (тир). Для того, чтобы растянуть зону объёмного звука на большее расстояние (для тренировок оперативных групп из нескольких сотрудников) была найдено техническое решение – шестиканальная система 5+1.

В качестве записей звуков предлагаются записи фильмов DVD-формата. DVD-фильмы обладают высокой стоимостью, но тем не менее следует признать что на DVD формируется объёмный звук очень высокого качества, записанный по стандарту Dolby Digital (AC-3 Digital), он обеспечивает шесть (пять + один) звуковых каналов. В большинстве современных фильмов звуковой ряд записан в стандарте AC-3 5.1 channels, то есть им обеспечивается пять отдельных (дискретных) каналов и один общий низкочастотный канал, которые рассчитаны на то, что перед человеком расположены три колонки (левая, правая и центральная), за его спиной расположено ещё два твитера (левый и правый), а в произвольном месте расположен сабвуфер (низкочастотная колонка). Воспроизведение звука с применением технологии AC-3, позволяет добиться того, что у человека создается полное ощущение реальности происходящих действий. Дискретная сущность звука Dolby Digital обеспечивает дополнительную чёткость звучания и эффект «объёмного пространства». Звук записанный по стандарту AC-3, может распространяться по помещению в произвольных направлениях в результате достигается «эффект присутствия».

Для воспроизведения столь сложного звука необходимы AC-3 декодер и шестиканальный усилитель, а также комплект колонок. Для технической реализации целесообразно применять следующие устройства:

Jazz speakers J9932, представляют недорогой AC-3 декодер с шестиканальным усилителем и комплектом колонок; *Genius SoundMaker Live! 5.1* – карта с программным декодированием AC-3. Она способна работать как настоящий AC-3 декодер.

Реализованный таким образом аппаратно-программный комплекс на базе PC IBM позволит в полном объёме обеспечить создание необходимого акустического фона при проведении практических занятий с сотрудниками ОВД по стрельбе и тактико-специальной подготовке.

В.Н. Лопатин, д-р юрид. наук, проф.

Правовые проблемы обеспечения информационной безопасности на региональном уровне

Несмотря на принятие Доктрины информационной безопасности РФ (2000) в решении вопросов её правового обеспечения мы, по сути, топчемся на месте. В Государственной Думе России ликвидирован подкомитет по законодательству в сфере информационной безопасности Комитета по безопасности, созданный в 1996 году. Ранее разработанные проекты, как новых законов, так и по внесению изменений в действующее законодательство, также как и концепция его развития, одобренная в 1998 году, остаются во многом нереализованными. Вместе с этим дальнейшее затягивание решения этих вопросов может оказаться тяжёлой преградой на пути прогресса в развитии информатизации и построения безопасного информационного общества. Из множества проблем выделим некоторые, требующие научного осмысления и разрешения на методологическом уровне.

Проблема разграничения полномочий. В соответствии с Конституцией Российской Федерации вопросы безопасности (п. «м» ст. 71), вопросы информации и связи, правового регулирования интеллектуальной собственности, (п.п. "и", "о" статьи 71) отнесены к ведению Российской Федерации. В то же время, вопросы защиты прав и свобод человека и гражданина, прав национальных меньшинств, обеспечения законности, правопорядка и общественной безопасности, обеспечения экологической безопасности, защиты семьи, материнства и детства, социальной защиты, осуществления мер по борьбе с катастрофами, стихийными бедствиями, эпидемиями и ликвидации их последствий, административного и административно-процессуального законодательства, кадров судебных и правоохранительных органов, защиты исконной среды обитания малочисленных этнических общностей, (п.п. «б», «д», «ж», «з», «к», «л», «м» статьи 72 Конституции РФ) находятся в совместном ведении РФ и субъектов РФ.

Налицо определённая коллизия конституционных норм, требующая теоретико-правового осмысления и законодательного разрешения. К сожалению, за 8 лет существования современной Конституции РФ эта проблема не разрешена ни на концептуальном, ни на законодательном уровне. Простым вычитанием из безопасности федерального уровня вопросов общественной и экологической безопасности, прямо отнесённых Конституцией РФ к совместному ведению РФ и её субъектов, эту проблему не решить. Это связано с понятием безопасности и

его закреплении в российском законодательстве. Сегодня общеизвестна формула безопасности, закреплённая с 1992 г. в Законе РФ «О безопасности» как «состояние защищённости¹ жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Исходя из этого, к основным *объектам безопасности* относятся: личность (её права и свободы), общество (его материальные и духовные ценности), государство (его конституционный строй, суверенитет и территориальная целостность). Одновременно с этим государство, организации и граждане относятся и к *основным субъектам* обеспечения безопасности. Главную роль при этом играет государство, которое в соответствии с действующим законодательством должно обеспечивать безопасность каждого гражданина, а также социальную и правовую защиту граждан и организаций, оказывающих содействие в обеспечении безопасности в соответствии с законом.

В Концепции национальной безопасности РФ (в ред. от 10 января 2000 г.) существенно дополнены и конкретизированы положения, ранее закреплённые в Законе РФ «О безопасности» (1992), что предопределяет необходимость их последующего подтверждения в новом Федеральном законе «О национальной безопасности». Приведём краткий сравнительный анализ этих отличий и изменений, поскольку они касаются как объектного и субъектного состава обеспечения безопасности, так и отношений, возникающих при этом. Если в Законе 1992 г. шла речь только о жизненно важных интересах, как совокупности потребностей, удовлетворение которых надёжно обеспечивает существование и возможности прогрессивного развития личности, общества и государства, то в Концепции введено понятие национальных интересов как совокупности сбалансированных интересов личности, общества и государства.

Интересы личности определены в Концепции как полное обеспечение конституционных прав и свобод, личной безопасности, повышение качества и уровня жизни, физическое, духовное и интеллектуальное развитие. Интересы общества установлены в упрочении демократии, создании правового государства, достижении и поддержании

¹ Смысл слова «защищать» отражает одну из важнейших функций безопасности, но не исчерпывает их. Представители Института социально-политических исследований РАН считают, что *безопасность* есть деятельность людей, общества, государства, мирового сообщества народов по выявлению (изучению), предупреждению, ослаблению, устранению (ликвидации) и отражению опасностей и угроз, способных погубить их, лишить фундаментальных материальных и духовных ценностей, нанести неприемлемый (недопустимый объективно и субъективно) ущерб, закрыть путь для выживания и развития.

общественного согласия, духовном обновлении России. Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии международного сотрудничества.

При этом ограничен (хотя и условно) перечень областей, национальные интересы в которых определяют предмет национальной безопасности: в области экономики, в социальной, внутривнутриполитической, международной, информационной сферах, в области военной (оборонной), пограничной и экологической безопасности. В целом, этот перечень соответствует существующему ныне перечню постоянных межведомственных комиссий Совета Безопасности Российской Федерации согласно утвержденной классификации компонентов безопасности, определяемых Законом РФ «О безопасности» и Положением о Совете Безопасности Российской Федерации. Появление трёх новых компонентов безопасности (социальная, внутривнутриполитическая, пограничная) соответствует норме Закона, предусматривающей возможность «иных видов безопасности», кроме прямо указанных в Законе, но повлечёт за собой реорганизацию МВК СБ РФ, в том числе решение вопроса об отнесении комиссии по охране здоровья населения, по-видимому, к социальной безопасности; специальной межрегиональной комиссии, комиссий по общественной безопасности, по борьбе с преступностью и коррупцией - к внутривнутриполитической безопасности.

Наряду со справедливым уточнением «принципы обеспечения безопасности» (в Законе - принципы безопасности) состав и содержание принципов существенно скорректированы. Так в Концепции национальной безопасности по ряду принципов, закреплённых в Законе РФ «О безопасности», раскрыто их содержание:

законность (соблюдение Конституции Российской Федерации, законодательства Российской Федерации и норм международного права при осуществлении деятельности по обеспечению национальной безопасности); соблюдение баланса жизненно важных интересов личности, общества и государства (единство, взаимосвязь и сбалансированность всех видов безопасности, гибкое изменение их приоритетности в зависимости от ситуации); не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных законом (уважение прав и свобод человека);

ряд принципов не нашли отражения в Концепции, хотя закреплены в Законе (взаимная ответственность личности, общества и гос-

ударства по обеспечению безопасности; интеграция с международными системами безопасности);

добавлены новые принципы обеспечения безопасности (приоритет политических и экономических мер обеспечения национальной безопасности с опорой на военный потенциал России; *сочетание централизованного управления силами и средствами обеспечения безопасности с передачей в соответствии с федеративным устройством России части полномочий в этой области органам государственной власти субъектов Российской Федерации и органам местного самоуправления*).

Кроме того, существенно скорректированы основные задачи по обеспечению национальной безопасности РФ, а также направления и полномочия государственных органов по формированию и реализации политики обеспечения национальной безопасности (Президент РФ, Федеральное Собрание РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти и органы исполнительной власти субъектов РФ).

Ответственность за нормотворчество и его результаты в законодательстве и практике правоприменения по вопросам информационной безопасности лежит, прежде всего, на федеральных органах государственной власти. Анализ действующего законодательства в сфере безопасности выявил его принципиальные недостатки: противоречивость, декларативность, наличие «белых пятен». Государство, не справляясь в полном объёме с задачей обеспечения безопасности всех субъектов, вынуждает их самостоятельно реализовывать свои интересы и защищать свои права всеми способами, не запрещенными законом, в соответствии с конституционным принципом самозащиты. Однако государство в большинстве случаев, не определив эти запреты по закону, пытается в лице различных структур (чиновников) *разрешать* такую защиту в каждом конкретном случае. Такой подход лишает граждан и организации уверенности в завтрашнем дне, что в итоге не позволяет решать проблемы. Необходимо чётко определить долю и границы государственного участия в обеспечении безопасности, в том числе через законодательное установление запретов и ограничений в информационной сфере.

Примером может служить ситуация с обеспечением охраны и защиты интеллектуальной собственности. В соответствии с Положением о Роспатенте, утверждённом Постановлением Правительства РФ от 19.09.97 г. № 1203 Роспатенту было поручено участвовать в разработке предложений по формированию государственной политики в сфере промышленной собственности. Ему же было поручено обеспе-

чивать охрану промышленной собственности. В соответствии с постановлением Правительства РФ от 12 апреля 1999 г. № 413 «О совершенствовании деятельности федеральных органов исполнительной власти в области авторского права и смежных прав» на Роспатент возложены функции по совершенствованию законодательства, международного сотрудничества и взаимодействия с общественными организациями в области авторского права, смежных прав, имеющим межведомственный характер. Указом Президента РФ от 2 августа 1999 г. № 954 в Положении о министерстве юстиции Российской Федерации (пункт 46) на министерство юстиции РФ возложены функции, аналогичные функциям Роспатента (совершенствование законодательства в области авторского права и смежных прав, взаимодействие с общественными объединениями, участие в международном сотрудничестве). Подобное положение привело к тому, что двум федеральным органам исполнительной власти поручены тождественные функции. Если при этом учесть, что аналогичные функции в отношении интеллектуальной собственности вменены также Минпромнауки РФ, Минимущество РФ, за их получение и осуществление борются ещё ряд ведомств, то на практике это может привести и приводит к дублированию решений, их противоречивости и другим негативным последствиям.

К сожалению, следует признать, что эту ситуацию не разрешили, а усугубили как Общеправовой классификатор отраслей законодательства, утверждённый Указом Президента РФ от 16 декабря 1993 г. № 2171, так и Классификатор правовых актов, утверждённый Указом Президента РФ от 15 марта 2000 г. № 511. В первом случае в 1993 г. была выделена как самостоятельная отрасль российского законодательства - законодательство о безопасности (350.000.000), в состав которого наряду с общими вопросами безопасности, вопросами статуса органов безопасности, внешней разведки включено и законодательство о государственной тайне. Во втором случае в 2000 г. там выделена как самостоятельная отрасль в 160.040.030 - безопасность и охрана правопорядка. *В то же время, например, информационная безопасность отнесена только к безопасности общества, тогда как к безопасности государства отнесена государственная тайна, являющаяся объектом защиты в системе информационной безопасности, а безопасность личности по данному Классификатору вообще оказалась за рамками информационной безопасности. В результате, вопросы информации и связи, правового регулирования интеллектуальной собственности, отнесённые по Конституции РФ к исключительной компетенции РФ, должны в соответствии с Указом Президента РФ*

от 15 марта 2000 года № 511 решаться в рамках обеспечения общественной безопасности, т.е. совместными усилиями РФ и её субъектов.

Нормотворчество в области информационной безопасности, на наш взгляд, можно отнести преимущественно к компетенции федеральных органов государственной власти, особенно, когда речь идёт о конфиденциальной информации. Институт тайны всегда используется для ограничения применения другого правового института – доступа к информации. Поскольку при этом всегда затрагиваются конституционные права и свободы в информационной сфере, то, в соответствии с частью 3 статьи 55 Конституции РФ **их ограничение может осуществляться только федеральным законом и только по основаниям, указанным в Конституции России.** В связи с этим, попытки законодательного регулирования этих вопросов на региональном уровне должны получать соответствующую оценку и реакцию органов прокурорского надзора, органов юстиции, осуществляющих регистрацию соответствующих актов, и судебных органов. Примером этого может служить принятие Новгородской Думой областного закона «Об информационных ресурсах Новгородской области», где в статье 16 «Конфиденциальная информация» региональный законодатель не только установил отличный от федерального порядок (в том числе критерии) отнесения информации к конфиденциальной, но и определил, что «контроль за соблюдением требований настоящей статьи осуществляет орган, специально уполномоченный губернатором области». Аналогичные попытки предпринимаются и в других регионах России, в т.ч. в г. Санкт-Петербурге.

Проблема разграничения компетенции государства и общества. Если в соответствии с Законом РФ «О безопасности» систему безопасности образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации, объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом (т.е. представлены все субъекты триады), то в Концепции национальной безопасности РФ основу системы обеспечения национальной безопасности РФ составляют органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства. В другом положении Концепции указывается, что национальные интересы России носят долгосрочный характер и обеспечиваются институтами государственной власти во взаимодействии с общественными организа-

циями, т.е. здесь граждане выступают лишь как объект безопасности, а участие общества ограничено общественными организациями.

До сих пор не решен вопрос и общественно-государственного участия в формировании и развития общественного правосознания. С упразднением государственной монополии КПСС, что было объективно необходимо, государство не взяло при этом на себя решение ряда важнейших функций, выполняемых ранее партией: кадровая политика (подбор, подготовка и расстановка кадров), идеологическая работа. Запрет государственной идеологии, закреплённый затем в Конституции РФ, привёл к тому, что государство отказалось, а общество ещё не готово единолично и эффективно решать задачу формирования и воспитания человека и гражданина. Основной из серьёзных *социально-психологических проблем* для России является то, что в конце двадцатого столетия произошло разрушение прежней системы формирования ценностей при одновременном культивировании новых: героизация преступника, приоритет силы денег перед силой закона, приоритет силы кулака, жестокости и насилия перед силой ума и души, «культурное» потребление наркотиков и т.п. На прошедшем 25 сентября 2001 года Президиуме РАН Кудрявцев В.Н. – академик РАН подчеркнул, что за последние 10 лет для большинства российских граждан приоритетами вместо порядка в государстве и спокойной совести стали личный успех и предприимчивость, 30-40 % опрошенных исповедуют сегодня индивидуализм западного типа, 15 % - приверженцы коллективизма, а 53 % - хотели бы жить как все. Такая категория людей, которые говорят одно, а делают другое, получила наибольшее распространение, особенно среди молодежи, что дало основание Леваде Ю. – директору ВЦИОМ придти к выводу, что появился «человек лукавый». Популярными стали лозунги типа «Любая работа хороша, если она даёт хороший заработок!» и принцип «Чего изволите?».

В соответствии с теорией развития «Я» Э. Эриксона, теорией гуманистической психологии А. Маслоу и теорией нейрологических уровней Г. Бейтсона у каждого человека в возрасте с 6 до 19 лет происходит формирование ценностей и убеждений, потребностей признания и почитания; формирование компетентности, верности выбранным идеалам, идентификация и самоутверждение; поиск ответов на вопросы «Почему?» и «Кто Я?». Главную роль в этих процессах обычно играют школа и система идеологического воздействия. Формирование системы взглядов сегодняшнего молодого поколения пришлось на годы перестройки и «смутного времени» (1985-2000 годы), когда государственная политика в этой области практически отсутствовала. Только в 1999 году Приказом Минобразования РФ № 19 от 28.09.99 г.

была утверждена государственная Программа развития воспитания в системе образования России на 1999-2001 годы.

Следует, по-видимому, признать ошибочным положение, ставшее нормой Конституции РФ (часть 2 статьи 13), что «никакая идеология не может устанавливаться в качестве государственной или обязательной». Государство как на федеральном, так и на региональном уровнях должно участвовать наряду с обществом в определении базовых, жизненно важных ценностей и их формировании, нести за это ответственность. Передача государственных функций должна происходить постепенно, по мере формирования гражданского общества и его готовности к решению этой важнейшей задачи.

Сегодня в органах прокуратуры из 30 тысяч прокурорско-следственных кадров 10 тысяч (34 %) - в возрасте до 30 лет, в том числе 14 % - горрайпрокуроры. В других правоохранительных органах, в том числе в милиции доля молодежи ещё выше. При этом, по данным психологов более половины всех поступающих на службу в милицию относятся к так называемой группе риска, то есть к лицам, служба которым в органах правопорядка противопоказана. Свыше 50 % выпускников вузов МВД России уходят из системы в первые пять лет службы. Средний стаж оперативника и следователя в ОВД составляет от трех до пяти лет.¹ Согласно прогноза ВНИИ МВД России к 2005 году руководящие позиции в иерархии МВД займут те сотрудники, которые в середине и в конце 90-х годов именовались «молодыми». Несформированная профессиональная самоидентификация, признание вынужденности выбора и выраженный меркантилизм существенно повышают вероятность возникновения установок на нарушение закона среди этой категории личного состава (которая к 2005 году приблизится к пику своей карьеры)².

В этой связи, следует признать хоть и запоздалым, но верным решение о введении института психологов в правоохранительных органах и придание их кадровым органам воспитательных функций. В то же время далеко не везде используются эти возможности достаточно эффективно. Например, только в 1/4 субъектов Российской Федерации

¹ Сальников В.П. Коррупция в органах внутренних дел: современное состояние и основные причины возникновения / Актуальные проблемы противодействия коррупции на региональном уровне: Сборник материалов научно-практической конференции Калининградский юридический институт МВД России. Калининград, КЮИ МВД России, 2001, с. 65.

² Проблемы укрепления законности в деятельности органов внутренних дел: Научно-практическое пособие / Под общ. Ред. В.Я. Кикотя. М.: ВНИИ МВД России, 2001, с. 34.

региональные прокуроры реализовали свое право в соответствии с Приказом Генерального прокурора РФ по введению в свой аппарат штатных психологов.

Эта особенность должна, безусловно, учитываться при профессиональной подготовке и воспитании кадров, в том числе в правоохранительных органах, при повышении их квалификации и работе с молодежью.

Проблема единого информационного пространства на региональном уровне. Сегодня во многих субъектах Российской Федерации принимаются свои региональные Концепции, законы, программы по построению единого информационного пространства в рамках своей административной территории. При этом разработчики и авторы этих документов нередко стоят на разных позициях, даже если они опираются в своей работе на принятые в этой сфере федеральные нормативные акты или делают ссылку на них.

Например, в Новосибирской области построение единого информационного пространства осуществляется в соответствии с Концепцией и Программой информатизации и создания единого информационного пространства Новосибирской области, а также областным законом «О функционировании единого информационного пространства Новосибирской области», подготовленными временной комиссией при Администрации области во исполнение распоряжения Главы Администрации области от 3 сентября 1996 г. № 519-р. Так, например, в перечисленном там составе объектов отсутствуют телекоммуникационные системы, хотя они указаны в объектном составе, данном в определении. Более того, это различие было закреплено там же ещё в одной статье, где записано, что закон регулирует отношения, возникающие в едином информационном пространстве при: формировании информационных ресурсов (сбор, обработка, накопление, хранение, поиск, защита, создание) и их использовании (передачу, распространение, предоставление); создании и использовании информационных технологий; защите информации и прав субъектов единого информационного пространства. Как видим, и здесь исключены из предметной области права в этой сфере отношения, возникающие в связи с созданием, развитием информационных систем и их защитой. Последнее обстоятельство крайне важно, так как защита информационных систем и отношения, возникающие в этой связи, являются также объектом права в области информационной безопасности наряду с защитой информации и защитой от информации основных субъектов этой сферы. Не учитывать это обстоятельство и необоснованно ограничивать число объектов

права в этой области общественных отношений — значит, на наш взгляд, допускать грубую методологическую ошибку.

Среди особенностей данной региональной концепции можно выделить как положительные, так и отрицательные моменты. Исходя из предложенной структуры информационного пространства, определены пять уровней информационной политики в России: государственный (федеральный); отраслевой; региональный; отдельного хозяйствующего субъекта; индивидуальный. В то же время в данной классификации отсутствует муниципальный уровень, что, на наш взгляд, неправильно, исходя из системного подхода в построении единого информационного пространства.

Хотя попытка характеристики информационных технологий в данном случае выгодно отличает документ от общероссийских концепций, в то же время она не учитывает в полной мере особенности применения отдельных современных технологий в открытых информационных системах и их возможные последствия.

К безусловным недостаткам данных документов относится то обстоятельство, что многие положения их прямо противоречат друг другу. Наряду с тем, что уже приводилось выше, приведём ещё один пример. Так, интеграция информационной среды Новосибирской области с единым информационным пространством России и мирового сообщества названа главным принципом региональной информатизации (здесь авторы отождествляют информатизацию с информационной политикой, что не совсем точно). В то же время первым из четырёх принципов функционирования единого информационного пространства области назван **приоритет интересов Новосибирской области**. Такой подход, когда каждый субъект системы заявляет о приоритете своих интересов, делает мало реализуемыми заявленные цели интеграции в единое информационное пространство, создает основу для возникновения внутренней угрозы этому процессу, что вообще, на наш взгляд, недопустимо в рамках единого государства. Под внутренней угрозой понимается возможность полного распада единого информационного пространства России, что означает возможность дальнейшего распада страны и утраты информационного суверенитета как важнейшего признака современной государственности.

Построение единого информационного пространства в г. Москве осуществляется на основе **Концепции городской политики** г. Москвы в области информатизации органов городского управления и началось в соответствии с Постановлением Правительства Москвы от 10 декабря 1991 года № 237, когда была утверждена Концепция создания и функционирования единой общегородской межведомственной

информационной системы. Тем самым был сделан первый шаг в реализации политики информатизации города по формированию единого информационного пространства. Распоряжением Мэра от 31 мая 1995 года № 576-РМ «Об упорядочении работ по информатизации московской городской администрации» были определены организационные меры по обеспечению создания информационных и автоматизированных систем в Комплексах городского хозяйства в рамках единой общегородской информационной системы. В ежегодных постановлениях Правительства Москвы по вопросам развития науки и технологий задачи информатизации города определены как основные в межотраслевых направлениях Городской программы. Главной целью городской политики в этой сфере также провозглашается - создание единого информационного пространства на основе системного подхода и общих принципов административных, организационных и технических решений по эффективному внедрению и использованию современных компьютерных технологий в сферу городского административного и хозяйственного управления.

Если в Новосибирской области в построении единого информационного пространства упор делается на развитие информационных технологий и ресурсов, то в Москве предпочтение отдается инфраструктуре – развитию информационных систем. Интересно, что в этих условиях хронического запаздывания федеральных властей по координации информационной политики региональные власти стали договариваться самостоятельно о взаимодействии в рамках межрегиональных ассоциаций в интересах создания единого информационного пространства. Примером этого может служить и то, что в июне 1999 года Межрегиональная ассоциация экономического взаимодействия "Сибирское соглашение" (МАСС) приняла решение о формировании единого информационного пространства в сфере производства и реализации продукции и финансовых потоков на территории 19 субъектов федерации - членов ассоциации. Это решение было продиктовано необходимостью более полного задействования производственного потенциала восточных регионов России, усиления деловой активности с одновременным использованием информации для рационального налогообложения¹.

Особенности участия муниципалитета в построении единого информационного пространства **на муниципальном уровне** рассмот-

¹ РосБизнесКонсалтинг. Выпуск 24 июня 1999 г.

рим на примере Концепции информатизации города Перми¹, где в качестве конечной цели развития информационной технологии управления городом заявляется формирование сотового информационного пространства города, которое должно стать частью единого информационного пространства государства (правда, в концепции затем эти понятия употребляются в обратном порядке – единое информационное пространство города и сотовое информационное пространство государства). Содержание объектного состава в этой концепции отличается от содержания объектов, приведённого в федеральных и региональных концепциях построения единого информационного пространства.

Так, создаваемая автоматизированная информационная система города (АИС), как основа единого информационного пространства и совокупность информационных систем города должна реализовываться на пяти уровнях:

- первый уровень, в виде автоматизированных рабочих мест (АРМ) с использованием одного компьютера;
- второй уровень, в виде локальных вычислительных сетей (ЛВС), связывающих от двух до нескольких десятков и сотен компьютеров (рабочих станций) и периферийные устройства в пределах ограниченной территории в единое целое с целью разделения доступа к общим ресурсам и взаимного обмена информацией, как правило, отраслевого характера;
- третий уровень, в виде муниципальной геоинформационной системы города;
- четвёртый уровень, в виде корпоративной информационной системы города;
- пятый уровень - интеграция в международные компьютерные сети Internet, FreeNet и сотовое информационное пространство России.

Перечисленные уровни, по-видимому, можно рассматривать и как определённые этапы построения единого информационного пространства. В состав городской информационной сети предлагается включить городской информационный центр, глобальные городские сети, базы данных общего пользования, локальные вычислительные сети структурных подразделений, службы поддержки.

¹ Авторский коллектив: Шавевич Г.А. - член-корреспондент МАИ; Соловьев В.Э. - член-корреспондент МАИ, канд. техн. наук; Низамутдинов О.Б. зав. кафедрой АСУ Пермского государственного технического университета, академик МАИ, д-р техн. наук, Концепция информатизации города Перми. Пермь, 1999.

Авторы Концепции включили в содержание инфраструктуры и информационные системы, и информационные ресурсы. Такой подход, возможный в технических решениях и проектах, с правовой точки зрения представляется неприемлемым. Ошибочным следует признать и подход к признанию муниципальными информационными ресурсами и муниципальной собственностью таких ресурсов, как базы персональных данных в автоматизированной системе учёта населения г. Перми (АСУН), предназначенной для сбора, хранения и ведения данных о каждом жителе города. Это, тем более не допустимо, что пользование такой информацией предполагается на основе городских соглашений между службами города о регламенте права собственности на обмениваемую информацию, информационные услуги, программную продукцию и т.д.

К принципиальным недостаткам можно отнести и отсутствие в документе положений о важном промежуточном звене интеграции в единое информационное пространство страны - единое информационное пространство региона (в данном случае - Пермской области).

Таким образом, несмотря на принятые федеральные нормативные акты, где заявляются основы и общие подходы к построению единого информационного пространства страны, в разных регионах и на разных уровнях сохраняются при всех отличиях в понятиях и названиях принципиальные особенности в подходах к построению единого информационного пространства на территории отдельного региона, муниципалитета (основные объекты, структура, принципы и приоритеты политики – в разных регионах разные не только по отношению к федеральным проектам и решениям, но и между собой). Очевидно, что здесь крайне важна функция координации усилий в регионах в этой сфере, с которой федеральный центр сегодня явно не справляется. При этом, региональным проблемам информационного обеспечения вертикали управления, защиты информационных ресурсов и решения информационно-правовых проблем демократизации общественной жизни на местах должно быть уделено особое внимание, необходимо учитывать реальную неравномерность процессов информатизации по регионам страны. Достаточно указать, что две трети всех используемых в стране баз данных приходится на четыре региона (Северо-Западный, Центральный, Уральский и Западно-Сибирский).

Таким образом, если в вопросах нормотворчества в области обеспечения информационной безопасности главную и исключительную роль играют федеральные органы государственной власти, а региональные структуры власти участвуют в этом, в основном, в пределах

делегированных полномочий; в формировании и развитии общественного правосознания федеральные и региональные органы власти должны участвовать и нести ответственность за это наряду с обществом, то в правоприменительной практике обеспечения информационной безопасности нужна координация региональных усилий на федеральном уровне.

В.А. Михайлов

Новые горизонты виртуальных технологий

В качестве основания для новой программы научно-исследовательской деятельности кафедры информационных систем Санкт-Петербургского университета МВД России предполагает использовать репутацию и авторитет, приобретённые Консорциумом Web3D в процессе экспертиз стандартов трёхмерных изображений по Internet. В том числе руководство кафедры собирается рассматривать предложения, поступающие от фирм-участников Консорциума, в целях выявления новых универсальных форматов. Конечной целью этой работы должен стать новый стандарт X3D, объединивший в себе все наиболее привлекательные стороны уже существующих.

Это чудо начала нового столетия, как утверждает президент Консорциума Web3D Нейл Треветт, формируется в условиях успешной стандартизации VRML 97. Кроме этого, теперь Консорциум Web3D уполномочен рассматривать любые предложения по внедрению интерактивного 3D на Web. Всё это говорит о том, что в недалеком будущем появятся не только более совершенные форматы и браузеры, но и новые графические ускорители и адаптеры, предназначенные именно для работы с виртуальной реальностью. Однако, пока всё это случится, для уже хорошо знакомого всем VRML наступает золотой век.

А тем временем прекращены работы по модернизации браузера CosmoPlayer, и его последняя версия - 2.1.1 - превратилась в финальную. К сожалению, произошло это не потому, что технология исчерпала свои возможности, а в связи с коммерческими неурядицами. Но и здесь все не так уж плохо, так как подобными разработками занималась не одна только Cosmo. И если у вас есть Pentium III или хорошая видеокарта, то, переключившись в параметр визуализации Render98, вы наконец забудете о надоедливых подвисаниях и скачках в процессе перемещения. А благодаря действительному присутствию в дистрибу-

тиве Cortona Active X компонента она может быть использована в любых самостоятельных приложениях. Кстати, программистами этой компании выпущен новый продукт - Internet Scene Assembler, предназначенный для удобной интерактивной анимации.

Что же касается 3D-чатов, то и здесь новая версия программы клиента Islands предлагает всем заинтересованным пользователям принять участие в освоении трёхмерных виртуальных пространств. Здесь вы сможете управлять 3D-объектами в многопользовательском режиме; обмениваться текстовыми сообщениями, даже загружать и просматривать свои собственные сцены и объекты. Причём требования к компьютеру самые гуманные: компьютер не менее Рентинум/133МГц/32Мб; ОС MS Windows95/98, MS Windows NT 4.0; на компьютере должен быть установлен MS Internet Explorer Ver. 3.02 и выше; объём программы клиента Islands около 2.8Мб.

В.А. Михайлов;

Г.И. Кожевников, канд. техн. наук

Принципы обеспечения безопасности интеллектуальных объектов

Проблемы обеспечения безопасности, защиты конфиденциальной информации, контроля доступа, автоматизации внутренних систем жизнеобеспечения объектов и централизации управления этими процессами в настоящее время в той или иной мере стоят перед организациями любых форм собственности и видов деятельности.

Работа в области системной интеграции предполагает полный комплекс услуг по консалтингу, разработке и внедрению интегрированных информационно-вычислительных систем. Используя многолетний практический опыт в области разработки комплексных систем, специалисты крупнейших вузов и компаний Санкт-Петербурга создали ряд собственных высокотехнологических продуктов, ориентированных на отечественных потребителей и во многом превосходящих по своим характеристикам известные зарубежные аналоги. Одним из таких продуктов является комплексная система безопасности и жизнеобеспечения интеллектуальных объектов.

Каждый проект по внедрению системы начинается с консалтингового исследования, в ходе которого проводится анализ объекта и потребностей клиента, на его основе разрабатывается техническая политика безопасности и жизнеобеспечения. После информационного и функционального моделирования разрабатывается техническая модель

системы безопасности и жизнеобеспечения. Планируются также восстановительные работы в случае возникновения чрезвычайных ситуаций. Таким образом, в ходе исследования изучаются потребности конкретного клиента, в связи с чем в проект вносятся изменения и дополнения.

Одним из самых перспективных направлений развития систем обеспечения внутренней безопасности, а также систем контроля доступа в выделенные помещения или зоны, является использование различных решений, основанных на применении в качестве персонального идентификатора пластиковых карт: микропроцессорных смарт-карт, карт радиочастотной идентификацией (проксимити-карт) или совмещённых. При помощи персонального идентификатора в виде пластиковой карты осуществляется разграничение доступа к внутренним информационным ресурсам объекта, к доступу в здания и внутренние помещения, а также к регулировке систем жизнеобеспечения.

Организация комплексной корпоративной системы на базе пластиковых карт с использованием единого информационного пространства гарантирует возможность централизованного контроля и управления внутренними системами объекта, обеспечивает оперативное взаимодействие всех звеньев системы между собой и позволяет работать системе в автономном режиме.

В рамках этого проекта устанавливаются системы обеспечения безопасности объекта, системы жизнеобеспечения и защиты информации. Управление подсистемами и компонентами комплекса осуществляется с нескольких автоматизированных рабочих мест (АРМ), объединённых в специализированную информационную сеть объекта.

В настоящее время автоматизированные системы контроля доступа являются перспективным решением для автоматизированного управления доступом сотрудников и транспорта на территорию, а также в здания и помещения административных учреждений, банков и организаций различных форм собственности. Применение автоматизированных систем контроля доступа на современном уровне и с минимальными затратами позволяет наряду со своими основными функциями обеспечить автоматизированный табельный учёт, уменьшить вероятность утечки конфиденциальной информации и хищения материальных ценностей.

Как отмечалось ранее, в качестве персонального идентификатора всё чаще используются пластиковые карты. Для графической персонализации карт сотрудников и клиентов в составе автоматизированной системы контроля доступа используется специализированная си-

стема цветной печати на пластиковых картах. При персонализации карт на каждую из них могут наноситься следующие данные:

- логотип учреждения или предприятия;
- фотографии сотрудника;
- фамилия, имя и отчество;
- подразделение и должность;
- специальные графические символы.

Возможно использование карты в качестве обычного пропуска на проходной.

В рамках проекта также предлагаются современные системы, предназначенные для защиты конфиденциальной информации от несанкционированного доступа в процессе её создания, обработки, хранения и передачи в информационных системах. Системы защиты информации обеспечивают организацию многоуровневого доступа к информационным ресурсам автоматизированных систем посредством разграничения назначенных каждому из пользователей прав по отношению к используемым им ресурсам локальных вычислительных сетей и персональных компьютеров, введением системы личных паролей и паролей доступа к библиотекам и базам данных, а также путём идентификации и последующей аутентификации пользователей. Предлагаются системы криптографической, антивирусной и Firewall защиты. Вся важная информация подвергается резервному копированию.

Система сигнализации является также одним из основных средств обеспечения безопасности любых объектов. Пожарная и охранная сигнализация по своему строению и применяемой аппаратуре имеют общие каналы связи, приёмы обработки информации и средства подачи тревожных сигналов.

Система обнаруживает любые изменения состояния охраняемых объектов и оповещает о характере этих изменений. В системах охранной и пожарной сигнализации возможно применение следующих типов датчиков: дымовых, температурных, контактных, магнитных, на разбитие стекла и объёмных.

Из всех технических средств безопасности, применяемых в настоящее время, системы видеонаблюдения являются одним из наиболее эффективных и экономически оправданных решений. Подобные системы предназначены для организации визуального автоматизированного наблюдения за охраняемой территорией и являются основным звеном интегрированных систем охраны. Они играют важную роль в комплексном обеспечении безопасности различных объектов - государственных учреждений, банков, офисов, торговых центров. Технические средства систем видеонаблюдения обеспечивают не только

непрерывный оперативный контроль за помещениями и территориями, но и отслеживают проникновение в охраняемые пространства, осуществляют запись тревожных событий, непрерывную видеозапись и многое другое.

Системы, предлагаемые учёными и разработчиками, являются результатом объединения последних достижений компьютерных технологий и разработок в области систем видеонаблюдения. Существующие системы видеонаблюдения достаточно разнообразны: от самых простых – одна камера на один монитор, до многокамерных, включающих в себя большое количество разнообразного оборудования.

Централизация управления и контроля за функционированием систем жизнеобеспечения объекта даёт массу преимуществ. Преимущество подобной централизации в способности принимать наиболее приемлемые и рациональные решения при возникновении неадекватных ситуаций, а также в возможности оперативного вмешательства в нормальное и аномальное функционирование систем без привлечения значительных человеческих и временных ресурсов. Система обеспечивает объективную регистрацию всех данных, необходимую для последующего анализа работы в произвольно выбранный промежуток времени.

М.В. Немцев;

Н.В. Бугель, д-р юрид. наук, проф.

Информационные войны

Информационное противоборство ранее присутствовало практически во всех войнах в таких основных формах, как ведение разведки и противодействие ей, распространение дезинформации, слухов и борьба с ними (в том числе при помощи цензуры) и т.п. С появлением новых информационных технологий и организацией международного информационного обмена на новом уровне информационная составляющая в стратегии обеспечения национальной безопасности, по оценкам Совета Безопасности Российской Федерации, руководителей российских спецслужб и Минобороны России, вышла на первый план. По данным ФАПСИ, за последние 15 лет расходы на приобретение средств информационной борьбы увеличилось в США в четыре раза, и занимают там сейчас первое место среди всех программ по вооружению. В интересах обеспечения информационной безопасности Америки Пентагон выделил на 1999г. 90 млн. долл. для проведения экспери-

ментальных исследований по ряду направлений, в том числе по созданию новых технологий распознаванию образов, формированию электронного образа боевого пространства, автоматическому поиску, сбору и обработке информации с помощью спутников. Информационное противоборство в ходе ведения обычной войны начало переходить на новую, более высокую стадию – информационной войны. Термин «информационная война» появился в середине 80-х годов в связи с новыми задачами Вооружённых Сил США после окончания «холодной войны» (разработка группы военных теоретиков США в составе Эклз Г., Саммерз Г. и др.); начал активно употребляться после проведения операции «Буря в пустыне» в 1991 году, когда новые информационные технологии впервые были использованы как средства ведения войны; официально впервые закреплён в директиве Комитета начальников штабов Вооружённых Сил США Т9 3600. 1. (декабрь 1992 года); детально разъяснён в Меморандуме № 30 (1993 год) заместителей министра обороны и председателя Комитета начальников штабов Вооружённых Сил США. В военных кругах США под информационной войной понимают действия, предпринимаемые для достижения информационного превосходства в поддержке национальной стратегии посредством воздействия на информацию и информационные системы противника.

К особенностям информационной войны можно отнести следующие:

расширяет территорию и пространство ведения войн, ведётся как при объявлении войны, так и в кризисных ситуациях в различных сферах жизнедеятельности;

ведётся как специализированными военными, так и гражданскими структурами.

Концепция «информационной войны», по оценкам российских спецслужб, предусматривает:

подавление (в военное время) элементов инфраструктуры государственного и военного управления (поражение центров командования и управления);

электромагнитное воздействие на элементы информационных и телекоммуникационных систем (радиоэлектронная борьба);

получение разведывательной информации путём перехвата и дешифрования информационных потоков, передаваемых по каналам связи, а также по побочным излучениям и за счёт специально внедрённых в помещения и технические средства электронных устройств перехвата информации (радиоэлектронная разведка);

осуществление несанкционированного доступа к информационным ресурсам (путём использования программно-аппаратных средств прорыва систем защиты информационных и телекоммуникационных систем противника) с последующим их искажением, уничтожением или хищением либо нарушением нормального функционирования этих систем («хакерная» война);

формирование и массовое распространение по информационным каналам противника или глобальным сетям информационного взаимодействия дезинформации или тенденциозной информации для воздействия на оценки, намерения и ориентацию населения и лиц, принимающих решения (психологическая война);

получение интересующей информации путём перехвата и обработки открытой информации, передаваемой по незащищённым каналам связи, циркулирующей в информационных системах, а также публикуемой в средствах массовой информации.

Оценка основных направлений ведения информационной войны подтверждается выделением в программах Университета национальной обороны США таких форм информационной войны, как радиоэлектронная борьба, война с использованием средств разведки, психологическая война, война с хакерами, кибернетическая война. В США проведены и осуществляются следующие основные мероприятия.

Создана объединённая комиссия по безопасности, которая с июня 1993 года по февраль 1994 года исследовала эту проблематику и пришла к выводу, что вторжение в информационные системы и сети - это важнейшая угроза безопасности в этом десятилетии и, вероятнее всего, в следующем столетии, что сети передачи данных превращаются в поле битвы будущего. Информационное оружие, стратегию и тактику применения которого ещё предстоит тщательно разработать. Оно будет использоваться с «электронными скоростями» и в обороне и в нападении. Информационные технологии позволят обеспечить разрешение геополитических кризисов, не производя ни одного выстрела. Политика обеспечения национальной безопасности и процедура её реализации должны быть направлены на защиту возможностей по ведению информационных войн и на создание всех необходимых условий для воспрепятствования противоборствующим США государствам вести такие войны.

Начата разработка стратегии подготовки и ведения информационных войн. Во всех видах Вооружённых Сил США созданы специализированные центры по ведению информационных войн:

Центр информационных боевых действий ВВС США – расположен в штате Техас на базе ВВС Келли;

Служба наземных информационных боевых действий Армии США - расположен в штате Вирджиния в форте Белвуар.

При этом в Пентагоне каждый из видов войск имеет свою рабочую группу по этой проблематике. В уставах Вооружённых Сил США и нормативных документах изложены принципы и способы ведения информационных войн.

Во всех видах Вооружённых Сил США созданы специальные подразделения ведения информационных войн и введены специальные должности офицеров. Во всех военных учебных заведениях введены спецкурсы по информационным войнам и идёт подготовка специалистов для ведения информационных войн (в 1995 году состоялся первый выпуск).

В Вооружённых Силах США проводятся учения и штабные игры по этой проблематике (опыт учений 1994-1995 годов обобщён в Пентагоне). Во время боевых действий за пределами США отрабатываются конкретные операции информационных войн с применением информационного оружия.

Проведено пять международных конференций по информационным войнам под эгидой правительства США.

Принимаются меры по ежегодному совершенствованию национальной информационной инфраструктуры, где по оценкам представителей правительства США, циркулирует до 80 процентов конфиденциальной информации, в том числе особо важной.

Ежегодно увеличиваются ассигнования на разработку новых видов информационного оружия (в Министерстве обороны, Агентстве национальной безопасности, ЦРУ США) и оснащением им национальных структур в объёме, превышающем, по оценкам экспертов, уровень затрат на ракетно-ядерные и космические программы 1994 года.

Информационное оружие, как и информационное противоборство, по мере развития общества и информационных технологий претерпевало изменения. В современной практике под информационным оружием, по определению американских экспертов, понимается комплекс программно-информационных средств, созданных для поражения информационных ресурсов противника.

Определение, данное российскими учёными и экспертами, представляется более точным.

Информационное оружие – это средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспреещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуни-

кационных сетей, компьютерных систем, всех средств высокотехнологического обеспечения жизни общества и функционирования государства.

Информационное оружие от обычных средств поражения отличает:

скрытность — возможность достигать цели без видимой подготовки и объявления войны;

масштабность — возможность наносить невосполнимый ущерб, не признавая национальных границ и суверенитетов, без привычного ограничения пространства во всех сферах жизнедеятельности человека;

универсальность — возможность многовариантного использования как военных, так и гражданских объектов страны поражения.

По оценкам Службы внешней разведки Российской Федерации, приведённым на парламентских слушаниях по теме «Угрозы и вызовы в сфере информационной безопасности», состоявшихся в Государственной Думе в июле 1996 года, сфера применения информационных войн включает как военную, так и экономическую, банковскую, социальную и иные области потенциального использования в целях:

дезорганизации деятельности управленческих структур, транспортных потоков и средств коммуникации;

блокирования деятельности отдельных предприятий и банков, а также базовых отраслей промышленности путём нарушения многозвенных технологических связей и системы взаиморасчётов, проведения валютно-финансовых махинаций и т.п.;

инициирования крупных техногенных катастроф на территории противника в результате нарушения штатного управления технологическими процессами и объектами, имеющими дело с большими количествами опасных веществ и высокими концентрациями энергии;

массового распространения и внедрения в сознание людей определённых представлений, привычек и поведенческих стереотипов;

вызова недовольства или паники среди населения, а также провоцирования деструктивных действий различных социальных групп.

При этом в качестве основных объектов применения информационных войн, как в мирное, так и в военное время выступают:

компьютерные и связные системы, используемые государственными организациями при выполнении своих управленческих функций;

военная информационная инфраструктура, решающая задачу управления войсками и боевыми средствами, сбора и обработки информации в интересах вооружённых сил;

информационные и управленческие структуры банков, транспортных и промышленных предприятий;

средства массовой информации, в первую очередь электронные (радио, телевидение и т.п.).

По своей результативности информационное оружие сопоставимо с оружием массового поражения. По оценке руководителей ФАПСИ «информационное оружие» сейчас является одной из основных угроз «информационной безопасности государства». На ежегодной конференции по этим проблемам в г. Таганроге в 1999 году были отмечены поражающие свойства информационного оружия и выработаны условия организации защиты от него, внесено предложение об организации совместных международных усилий по предотвращению информационных войн и ограничению оборота информационного оружия.

А.В. Никулин;

П.В. Бабарыкин

Использование современных информационных технологий в области автоматизированной оценки знаний

Одним из важных этапов процесса обучения является этап проверки и оценки знаний. Полученные в ходе проверки и оценки знаний результаты могут свидетельствовать о готовности или неготовности обучаемого к дальнейшему изучению того или иного предмета. Этап оценки знаний является ключевым при выборе дальнейшего направления обучения. Современные информационные технологии в области автоматизированной оценки знаний предоставляют преподавателю удобный инструмент для сбора, накопления, обработки и анализа оценки подготовленности обучаемых.

Одной из простейших форм автоматизированной оценки знаний является форма тестов, направленных на применение современных информационных технологий. Это представляется целесообразным в виду того, что творческое участие преподавателя фокусируется на подготовке и разработке тестовых заданий, а рутинная работа по опросу учащихся, сбору ответов и их количественному подсчёту осуществляется компьютерной программой. Кроме этого, в зависимости от качества проработки тестовых вопросов, тестовые задания отвечают та-

ким принципам оценки знаний как принципы полноты, всесторонности и объективности.

На сегодняшний день существует целый ряд компьютерных программ, реализующих функции автоматизированных систем оценки знаний в форме тестов. Одной из таких программ является «Компьютерная система тестирования», разработанная на кафедре информационных систем Санкт-Петербургского университета МВД России. Изначально в программу закладывался ряд особенностей, которые выделяют её из ряда подобных программ. Программа разработана на основе оригинальной идеи, учитывающей психологию принятия решений: каждый выбор сопровождается указанием самооценки степени уверенности отвечающего. Оценка результатов тестирования зависит от соотношения правильности ответов и степени уверенности в них. Эта идея позволила:

- увеличить шкалу оценок результата и получить существенную дифференциацию обучающихся, это дало возможность использовать не абсолютные, а относительные и порядковые оценки (рейтинговая оценка в анализируемой группе), ввести элемент соревнования и исключить подсказку одним учащимся другим;

- сократить возможности простого «угадывания» ответа и случайных ошибок (отвечающий имеет право на ошибку и может с некоторыми долями уверенности выбрать и все предложенные альтернативы);

- отказаться от метода простой альтернативы (среди вариантов ответов ровно один – правильный) и разрабатывать вопросы, среди вариантов ответов на которые могут быть и все правильные, и все неправильные.

Другим средством, позволяющим управлять процедурой оценивания в программе, является возможность определения весовых коэффициентов для вопросов, например, связанных с экспертной оценкой их сложности или приоритетности.

Важной составляющей при подготовке тестовых заданий является возможность использования в программе мультимедиа возможностей, то есть задавать представление вариантов ответов в виде картинки, аудио или видео фрагмента, что выгодно отличает проведение тестирования на компьютере от тестирования на бумаге.

Дальнейшее совершенствование программы «Компьютерная система тестирования» связано с улучшением пользовательского интерфейса, расширением возможностей использования современных мультимедиа технологий, а также добавлением опционального элемента обучения при тестировании. Элемент обучения в ходе тестирования

заключается в том, что после выполнения тестовых заданий, тестируемый сможет увидеть не только количественный результат правильных и неправильных ответов, но также и сами варианты ответов, что позволит ему определить, когда и почему была допущена ошибка.

Таким образом, применение современных информационных технологий в области автоматизированной оценки знаний позволяет существенным образом облегчить труд преподавателей, сфокусировать их внимание на разработке и подготовке тестовых заданий, а учащиеся получают возможность быстро проверить свои знания с целью самоконтроля или в ходе процессе самообучения.

А.В. Никулин;

М.Л. Тихомирова

Информационная безопасность в сфере частных интересов

Под безопасностью принято понимать состояние защищённости жизненно важных интересов от внутренних и внешних угроз. Жизненно важные интересы – это совокупность потребностей, удовлетворение которых надёжно обеспечивает существование и возможности прогрессивного развития личности, общества, государства¹. В соответствии с законом «О безопасности» от 5 марта 1992 года, личность её права и свободы относятся к основным объектам безопасности.

Современное развитие информационных технологий помимо ощутимых преимуществ принесло и негативные явления, открыв новые способы нарушения частных интересов и прав, в том числе гарантированных Конституцией РФ. Так, в соответствии со статьей 23 ч. 1, каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и личной жизни. Специфическими особенностями нарушения прав в данном случае будет обладать объективная сторона преступления: компьютер и/или сеть являются средством достижения цели.

Конкретно, нарушение прав может выступать в форме клеветы (ст. 129 УК РФ), оскорбления (ст. 130 УК РФ), нарушения неприкосновенности частной жизни (ст. 137 УК РФ), нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 139 УК РФ), нарушения авторских и смежных прав (незаконное использование объектов авторского права или смежных прав,

¹ Закон Российской № 2446-1 от 5 марта 1992 г «О безопасности».

а равно присвоение авторства, если эти деяния причинили крупный ущерб) (ст. 146 УК РФ), нарушения изобретательских и патентных прав (незаконное использование изобретения, полезной модели или промышленного образца до официальной публикации сведений о них, присвоение авторства или принуждение к соавторству, если эти деяния причинили крупный ущерб) (ст. 147 УК РФ), кражи (тайное хищение чужого имущества) (ст. 158 УК РФ), мошенничества (хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием) (ст. 159 УК РФ), вымогательства (требование передачи чужого имущества или приобретение права на чужое имущество или совершение других действий имущественного характера под угрозой применения насилия либо уничтожения или повреждения чужого имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить вред правам или законным интересам потерпевшего или его близких) (ст. 163 УК РФ), причинение имущественного ущерба путём обмана или злоупотребления доверием (ст. 165 УК РФ), умышленного уничтожения или повреждения имущества (если эти деяния повлекли причинение значительного ущерба), заведомо ложной рекламы (использование в рекламе заведомо ложной информации относительно товаров, работ или услуг, а также их изготовителей (исполнителей, продавцов), совершённое из корыстной заинтересованности и причинившее значительный ущерб) (ст. 182), незаконного получения и разглашения сведений, составляющих коммерческую или банковскую тайну, путём похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений.

Ввиду того, что частная информация конфиденциального характера нередко в силу закона или обстоятельств может или должна предоставляться в государственные органы или социальные организации различной принадлежности, то следует говорить об обеспечении информационной безопасности частных интересов на уровне частных лиц и на уровне государственных органов и организаций, куда гражданин предоставил сведения, не подлежащие огласке.

Рассматриваемая проблема не является российской спецификой. Так, три четверти американцев-пользователей Интернета обеспокоены проблемами в сфере информационной безопасности и почти столько же опасаются, что их информация частного характера может быть украдена или незаконно использована. Об этом говорят результаты опроса, проведённого Американской Ассоциацией Информационных

Технологий (Information Technology Association of America – ITAA) и корпорацией Tumbleweed Communications.

Тридцать пять процентов опрошенных говорят, что «они очень обеспокоены» проблемами информационной безопасности, тридцать шесть процентов, что они «в основном обеспокоены», 33 % респондентов утверждают, что они «очень сильно опасаются за свою частную информацию в Сети и 41 % «серьёзно опасаются».

78 % респондентов говорят что они «очень» или в «достаточной степени» опасаются незаконного использования своей персональной информации, предоставленной государственными органам.

Менее, чем 20 % уверены в способности государственных структур обеспечить безопасность частной информации и предотвратить направленные против них кибератаки, 54 % «в общем уверены» и 17 % опрошенных американцев «не верят в это совсем».

Традиционно существуют два пути обеспечения информационной безопасности: технический и юридический. И если первый носит превентивный характер, то второй путь, как правило, выполняет правовосстановительную функцию.

Одним из наиболее эффективных технических способов обеспечения информационной безопасности (внутри организации среднего масштаба) является применение сетевых экранов. По мнению западных экспертов, лучшими на сегодняшний день параметрами обладает аппаратный межсетевой экран WatchGuard Live Security System от компании WatchGuard Technologies (www.watchguard.com).

И, всё-таки, несмотря на приоритетность в данной сфере технических средств защиты информации, следует заметить, что обеспечение информационной безопасности является постоянно текущим процессом, и никакой даже самый совершенный сетевой экран не в состоянии обеспечить 100-процентную защиту от посягательства на информационные ресурсы. Грамотное построение системы информационной безопасности предполагает помимо использования технических средств, постоянное совершенствование законодательства и правоприменительной практики.

*Л.Г. Перфильев, канд. пед. наук, профессор;
П.В. Бабарыкин*

Правовая культура учащихся в области информационных отношений

Развитие современного общества неразрывно связано с процессом обмена информацией и появлением технических новинок для его улучшения. Технические средства позволяют получать огромное количество информации, зачастую больше, чем её может усвоить отдельный человек. Важным аспектом обмена информацией является то, как индивид воспользуется информацией, как превратит её в знание и получит социально значимый результат (социально полезный или социально вредный, преступный). Подобные навыки формируются изначально в процессе обучения и в последующем – самообучения. Качество образовательного процесса определяет направленность развития личности.

В условиях создания институтов информационного права и появления информационной культуры особую значимость приобретает формирование правовой культуры учащихся в сфере информационных отношений. Правовая культура личности отражается в уровне её правомерной деятельности. Данное обстоятельство свидетельствует о неразрывной связи правовой культуры учащегося с правовой культурой общества, которая состоит из правосознания, системы правовых актов и юридической деятельности. В связи с этим необходимо предусмотреть систему мер, направленных на положительное изменение различных элементов правовой культуры учащегося и правовой культуры общества.

На уровне школьного образования можно предложить следующие меры:

- включение правового воспитания в школьные программы обучения;
- повышение нравственно правовой культуры учащихся;
- развитие умений творчески использовать получаемую информацию для решения социально-правовых проблем, для защиты своих прав;
- формирование мировоззрения, основанного на системно-информационном подходе;
- переход от репродуктивной к продуктивной ориентации образовательного процесса;
- введение новых форм обучения (модульное обучение);

- и др.

В формировании правовой культуры школьника важную роль играет позиция родителей. Если они понимают значение правовой культуры и создают условия для её формирования, то процесс обучения становится двунаправленным и приносит пользу детям и их родителям.

В результате взаимодействия различных социальных институтов (семья, школа и т.д.) по реализации системы мер формирования правовой культуры учащихся в сфере информационных отношений направленность личности учащегося будет находиться в правовом поле, и, следовательно, социально значимые результаты их деятельности будут правомерными и законными, что является необходимой предпосылкой к формированию гражданского общества и правового государства.

Д.А. Петров, канд. юрид. наук, доцент

Правовые аспекты информационной безопасности должника в процессе по делу о банкротстве

Основой рыночной экономики является конкуренция товаров (работ, услуг), конкурентоспособность которых определяется не столько возможностью доступа предпринимателей к сырью и энергоресурсам, сколько использованием эффективных технологий, более современного оборудования, секретов производства, и др. Это позволяет произвести и предложить потребителям более экономичные товары (работы, услуги), чем у других аналогичных производителей. И, тем самым, вопросы обладания и пользования информационными ресурсами приобретают первостепенное значение.

Информация предпринимателя подразделяется на открытую (доступную всем) и закрытую (специально скрываемую и защищаемую предпринимателем от посторонних лиц). В условиях жесточайшей конкуренции информация, обеспечивающая предпринимателю стабильность и коммерческий успех, является, как правило, закрытой.

Правила, устанавливающие информационную безопасность должника в процессе по делу о банкротстве, объективно необходимы. И эти правила должны действовать уже на стадии принятия мер, направленных на предупреждение банкротства должника. Именно поэтому норма, запрещающая опубликование или разглашение иным образом сведений о банкротстве должника до момента публикации ре-

шения арбитражного суда о признании должника банкротом, помещена в главу 2 «Предупреждение банкротства» Закона о банкротстве¹. Но ни в коем случае это не ограничивает её действие исключительно этапом предупреждения банкротства.

Нормы, устанавливающие правила о предупреждении банкротства, привнесены в действующее законодательство Законом о банкротстве. Конечно, их немного. Но и детального регулирования здесь не требуется. Главное, дать сторонам толчок, предоставить возможность предупредить банкротство, не втягиваясь в дорогостоящий и длительный процесс по делу о банкротстве. И на этой стадии законодательство вводит в действие правила об информационной безопасности должника.

Хочется особо отметить, что нормы о предупреждении банкротства применяются не всегда. Скорее, от самого должника, кредитора, третьих лиц, зависит решение вопроса – применять их или нет. Нормы об информационной безопасности должника имеют другой правовой режим – они вводятся на стадии предупреждения банкротства вне зависимости от желания субъектов этого правоотношения с момента появления сведений о банкротстве должника.

С момента введения в действие, Закон о банкротстве не создавал особых препятствий для обращения в суд с заявлением о признании должника банкротом. Поэтому Конституционный Суд Российской Федерации указал², что до внесения необходимых изменений в Закон о банкротстве арбитражные суды на основании формальной проверки заявления о признании должника банкротом и представленных документов вправе вынести определение о принятии данного заявления, вопрос же о введении наблюдения должен решаться после получения от должника разъяснений и возражений на заявление и оформляться отдельным определением.

¹ Федеральный закон от 8 января 1998 г. № 6-ФЗ «О несостоятельности (банкротстве)» // Собрание законодательства Российской Федерации, 1998, № 2, ст. 222 (Здесь и в дальнейшем именуется как Закон о банкротстве).

² См. п. 2 Постановления Конституционного Суда РФ от 12 марта 2001 года 4-П «По делу о проверке конституционности ряда положений Федерального закона «О несостоятельности (банкротстве)», касающихся возможности обжалования определений, выносимых арбитражным судом по делам о банкротстве, иных его положений, статей 49 Федерального закона «О несостоятельности (банкротстве) кредитных организаций», а также статей 106, 160, 179 и 191 Арбитражного процессуального кодекса Российской Федерации в связи с запросом Арбитражного суда Челябинской области, жалобами граждан и юридических лиц // Российская газета, 2001, 22 марта.

Это предоставило должнику дополнительные гарантии, особенно в случаях недобросовестного поведения кредитора. Но факт остается фактом – принятие арбитражным судом к рассмотрению заявления о признании должника банкротом зачастую является фактором, изменяющим финансово-хозяйственную ситуацию, складывающуюся вокруг должника. В этих условиях контрагенты должника будут пересматривать характер своих отношений с должником, стараясь брать за основу конструкции товарного, коммерческого кредита, либо, по крайней мере, обуславливать исполнение своих обязательств встречным исполнением со стороны должника.

В этих условиях опубликование или разглашение иным образом сведений о банкротстве должника до момента публикации решения арбитражного суда о признании должника банкротом может привести к дестабилизации финансово-хозяйственной деятельности должника.

Именно поэтому Закон о банкротстве законодательно распространяет режим конфиденциальности информации на сведения о банкротстве должника. Необходимо отметить, что процесс по делу о банкротстве не исключает возможности использования гражданско-правового режима служебной и коммерческой тайны, устанавливаемого по инициативе должника. Но в этом случае, законодательно установленный режим конфиденциальности информации является более важным и подлежит приоритетному применению. Вне его правового поля может действовать обычный режим служебной и коммерческой тайны. Но именно законодательно установленный режим для нас наиболее интересен, поскольку его правила обязательны. В дальнейшем о нём и пойдёт речь.

Допустимо ли держать в неведении контрагентов должника, не афишируя сведения о его нестабильном положении? Несомненно, что сведения о банкротстве должника должны быть раскрыты при введении процедуры конкурсного производства. В соответствии с абз. 4 п. 1 ст. 98 Закона о банкротстве с момента принятия арбитражным судом решения о признании должника банкротом и об открытии конкурсного производства сведения о финансовом состоянии должника прекращают относиться к категории сведений, носящих конфиденциальный характер либо являющихся коммерческой тайной. Это позволит предъявить всем кредиторам соответствующие требования, провести мероприятия, предусмотренные конкурсным производством. Ну, а последующее опубликование сведений о признании должника банкротом и об открытии конкурсного производства, осуществляемое конкурсным управляющим за счёт должника в специальных изданиях (ст. 100 За-

кона о банкротстве), завершит процесс раскрытия информации о банкротстве должника.

Итак, механизм информационной безопасности должника Законом о банкротстве определён. Но работает ли он? Обеспечивается ли на практике информационная безопасность должника?

Часто мы встречаемся с тем, что после принятия арбитражным судом заявления о банкротстве должника и введения процедуры наблюдения в средствах массовой информации появляются сообщения об этом, особенно часто в отношении должников, достаточно значимых для экономики региона, бизнес которых интересен для конкурентов. Временный управляющий, внешний управляющий охотно дают интервью. Тем самым, сведения о банкротстве становятся всеобщим достоянием. Это является неправомерным, а лица, допустившие нарушение, несут ответственность, установленную федеральным законом.

В этой проблеме есть несколько аспектов:

Что понимается под сведениями о банкротстве должника?

На какой период времени сведения о банкротстве должника относятся к охраняемой информации?

В каких случаях возможно или необходимо раскрытие информации о банкротстве должника и в каком объёме?

Каковы аспекты ответственности за нарушение запрета о неразглашении сведений о банкротстве должника?

Закон о банкротстве, устанавливая запрет на распространение сведений о банкротстве должника в рамках мер по предупреждению банкротства, не определяет, что понимается под сведениями о банкротстве должника.

Косвенный ответ даёт ч. 2 ст. 100 Закона о банкротстве. Публикация сведений о признании должника банкротом и об открытии конкурсного производства должна содержать: наименование и иные реквизиты должника, признанного банкротом; наименование арбитражного суда, в производстве которого находится дело о банкротстве; дату принятия арбитражным судом решения о признании должника банкротом и об открытии конкурсного производства; срок, установленный на предъявление требований кредиторов, который не может быть менее двух месяцев с даты указанной публикации; сведения о конкурсном управляющем.

Но конфиденциальности этих сведений явно недостаточно для информационной безопасности должника. Перечень следует расширить, все сведения о финансово-хозяйственном положении должника признав конфиденциальной информацией. Но, по крайней мере, сведения о рассмотрении дела уже являются конфиденциальной информа-

цией. В категорию сведений о банкротстве должника включаются в качестве составляющей сведения о финансовом состоянии должника, поскольку они раскрываются с момента введения конкурсного производства (абз. 4 п. 1 ст. 98 Закона о банкротстве). Следовательно, до момента принятия решения о признании должника банкротом сведения о финансовом состоянии должника охраноспособны.

Закон о банкротстве установил, что с момента принятия арбитражным судом решения о признании должника банкротом и об открытии конкурсного производства сведения о финансовом состоянии должника прекращают относиться к категории сведений, носящих конфиденциальный характер либо являющихся коммерческой тайной.

Также обращает на себя внимание некоторая неопределённость в правовом режиме конфиденциальной информации и коммерческой тайны. Соответствующий закон пока не принят.

Следует отметить, что вопросы, связанные с защитой информации, имеющей ограниченный доступ, в том числе коммерческой тайны, регулируются Гражданским кодексом Российской Федерации (статьи 139, 727, 771 и 772) и другими законодательными актами Российской Федерации. Статья 139 Гражданского кодекса Российской Федерации, называющая служебную и коммерческую тайны в качестве объектов гражданских прав, подлежащих специальной охране, устанавливает, что законодательно могут быть решены только вопросы определения перечня сведений, которые заведомо не могут составлять коммерческую тайну, а также вопросы защиты коммерческой тайны.

Существует мнение¹, что открытие конкурсного производства влечёт утрату характера конфиденциальности любой информации о должнике. По нашему мнению, только после опубликования сведений о признании должника банкротом и об открытии конкурсного производства (фактически, по прошествии нескольких недель) информация о должнике должна утратить свойство конфиденциальности. Но и то, здесь не вся информация о должнике утрачивает характер конфиденциальной, а только та, которая была таковой признана Законом о банкротстве. Локально регулируемый режим служебной и коммерческой тайны всё равно сохранится. Другой вопрос, будет ли это актуально и востребовано в преддверии ликвидации должника?

В рамках реализации процедур банкротства будет происходить поэтапное раскрытие информации банкротстве должника. А к момен-

¹ Телюкина М.В. Комментарий к Федеральному закону «О несостоятельности (банкротстве)» / Отв. ред. проф. А.Ю. Кабалкин. – М.: Издательство БЕК, 1998. – 510 с.

ту, когда информация о финансовом состоянии должника утратит свойства конфиденциальной информации или коммерческой тайны (абз. 4 п. 1 ст. 98 Закона о банкротстве), она уже будет известна многим. По крайней мере, лица, заинтересованные в должнике, уже будут обладать ею.

Норма п. 3 ст. 26 Закона о банкротстве запрещает распространять сведения о банкротстве должника. До заинтересованных лиц эта информация доводится в соответствии с указаниями закона. А с момента опубликования сведений о признании должника банкротом они становятся общедоступными. Тем самым, законодательно установленный режим охраны информации снят.

Наиболее важным аспектом проблемы обеспечения информационной безопасности должника в процессе по делу о банкротстве является установление ответственности за несанкционированное раскрытие информации.

Закон о банкротстве определил, что лица, допустившие опубликование или разглашение иным образом сведений о банкротстве должника до момента публикации решения арбитражного суда о признании должника банкротом, несут ответственность, установленную федеральным законом.

В соответствии с нормами ст. 139 ГК РФ лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причинённые убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Но труднодоказуемость категории «убытки» общеизвестна. И при несанкционированном раскрытии конфиденциальной информации доказать убытки практически невозможно.

Президент Российской Федерации, отклоняя проект Федерального закона «О коммерческой тайне»¹ указал, что информация, составляющая коммерческую тайну, относится к объектам гражданских прав, то есть в отношении коммерческой тайны действуют соответствующие нормы Гражданского кодекса Российской Федерации, включая нормы о гражданско-правовой ответственности за её разглашение и использование. Но этого явно недостаточно.

¹ Письмо Президента РФ от 23 февраля 1999 г. № Пр-244 // Справочная правовая система «Гарант».

Поэтому, проект предусматривал, что обладатель коммерческой тайны самостоятельно определяет способы защиты своих прав на коммерческую тайну и вправе требовать: а) признания прав обладателя на коммерческую тайну; б) пресечения действий, нарушающих режим коммерческой тайны или создающих угрозу его нарушения; в) возмещение убытков, причинённых разглашением или неправомерным использованием коммерческой тайны; г) выплаты компенсации в размере от 50 до 50 тысяч минимальных размеров оплаты труда, установленных федеральным законом, по усмотрению суда в случае невозможности определения размера убытков вследствие нарушения прав на коммерческую тайну; д) заключения лицензионного договора или договора о передаче ноу-хау при наличии определённых условий и при фактическом использовании ноу-хау третьим лицом в своих интересах; е) принятие иных предусмотренных законодательством и обеспечивающих защиту его прав на коммерческую тайну мер.

По нашему мнению, наиболее действенным способом явилась бы выплата компенсации в случае невозможности определения размера убытков вследствие нарушения прав на коммерческую тайну¹. Но такого способа защита пока нет.

Итак, действующее законодательство должно быть реформировано и информационная безопасность должника в процессе по делу о банкротстве должна быть обеспечена.

А.И. Примакин, канд. техн. наук, доцент

Возможности скрытой передачи служебной информации при проведении оперативных мероприятий сотрудниками органов внутренних дел

Защите речевых сообщений конфиденциального характера уделяется в последние годы всё большее внимание. Свидетельством тому - многочисленные публикации в специализированных журналах².

Смысловая защита речевых сообщений посредством криптографических методов до сих пор рассматривалась специалистами как

¹ Аналогичный способ используется при защите прав автора в законодательстве об авторском праве и смежных правах.

² См., напр., Дворянкин С.В., Клочкова Е.Н., Калужин Р.В. Маскирование речевых сообщений на основе современных компьютерных технологий // Специальная техника, 2001, № 3, с. 43-51.

единственная возможность гарантированной или высоконадёжной защиты различных каналов речевой связи независимо от условий ведения переговоров, технических характеристик связной аппаратуры и других факторов.

Особенностью работы устройств цифрового засекречивания речи являются криптографические преобразования цифровых данных с последующей передачей в канале связи. Безопасность связи при передаче речевых сообщений, и, прежде всего, направление, обеспечивающее их смысловую защиту, основывается на использовании большого количества различных методов и средств преобразования аудио сигналов. Они меняют характеристики речи, делая её неразборчивой или неузнаваемой для подслушивающего лица, перехватившего обработанное речевое сообщение, или вообще, скрывая сам факт передачи конфиденциальной информации. Однако увеличение криптостойкости сообщения приводит к уменьшению пропускной способности аудио-канала (при условии неизменной общей пропускной способности канала) и при этом, в принципе, любая зашифрованная информация может быть раскрыта. Возможная скорость дешифровки речевых сигналов с учётом их важности, определяется финансовыми затратами, растущими экспоненциально при уменьшении времени раскрытия зашифрованной информации. Возникающее противоречие между оперативностью передаваемой информации и требуемой криптостойкостью сообщения ставит проблему обеспечения надёжной передачи служебной информации вместе с речью без ухудшения её качества.

Концептуальная постановка задачи по обеспечению безопасности речевых сигналов сводится к реализации в реальном времени скрытной передачи служебной информации без ухудшения качества речевого сигнала, его частотной полосы пропускания и отношения сигнал/помеха. Последнее означает, что пропускная способность канала при одновременной передаче речи и вспомогательных сигналов должна остаться прежней.

Достичь требуемого можно только «размещением» служебных сигналов без потери разборчивости речевого сообщения во время передачи. Тривиальным решением могла бы быть передача информации в специально выделенной полосе частот, но очевидно, что это привело бы к ухудшению качества передаваемой речевой информации. Пути решения данной проблемы необходимо искать в особенностях восприятия акустических сигналов слуховой системой человека.

Хорошо известно, что во внутреннем ухе человека имеется основная (базилярная) пластина, по которой звуковые волны передаются от её широкого конца у стремени (около барабанной перепонки) к её

узкому верхнему концу. До определённой точки за барабанной перепонкой по основной пластине могут пройти только те волны, частота которых ниже некой критической частоты $f_{кр}$. Эта верхняя критическая частота уменьшается по мере уменьшения ширины основной пластины. Таким образом, пройти весь путь от барабанной перепонки до узкого верхнего конца основной пластины могут только низкочастотные волны. Волны же большей части частотного диапазона испытывают отражение на своём пути по основной пластине. Основная пластина очень неупруга, в ней велики потери. В процессе отражения основная часть энергии поглощается, и отражённая волна оказывается очень слабой¹.

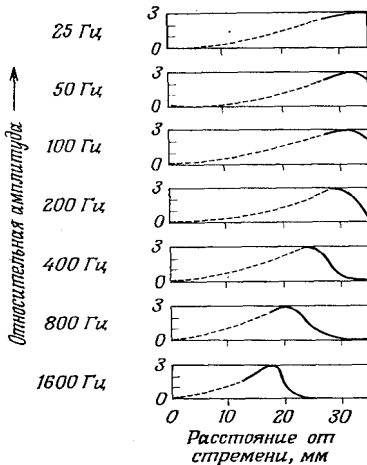


Рис. 1. Огибающая смещений в основной пластине внутреннего уха при разных частотах синусоидального напряжения, приложенных к стремени

На рис. 1 показана огибающая синусоидальной волны, бегущей по основной пластине слева направо. Эти графики взяты из работы². Здесь огибающая даёт амплитуду смещения в каждой точке по мере распространения волны. На данной частоте f напряжённость волны максимальна в месте отражения. При возрастании частоты это место приближается к стремени (барабанной перепонке). Таким образом, место наибольшей напряжённости волны зависит от частоты. С этой частотной зависимостью места отражения связана способность слуховой системы воспринимать частоту звука.

¹ Пирс Дж. Почти всё о волнах. М.: Мир, 1976, с. 176.

² Denes P.B., Pinson E.H., The Speech Chain, Bell Telephone Laboratories, 1963.

Таким образом, в слуховой системе человека акустические сигналы представляются в координатах масштаб-время, что соответствует представлению сигнала с помощью вейвлет-преобразования, т.е. улиточный механизм слуховой системы выполняет вейвлет-преобразование¹.

Известно, что вейвлет-представление сигнала обладает двойной симметрией относительно сдвига сигнала и преобразования сжатия-расширения. Этот факт позволяет утверждать, что при анализе речевых сигналов выгодно представлять сигнал в виде совокупности масштабов разной размерности. Действительно, при передаче речевой информации можно сначала передать низкочастотные составляющие, а затем последовательно передавать высокочастотные составляющие речи. Такая стратегия передачи имеет определённые выгоды. Так, при передаче речевых сигналов недопустимо изменять крупные масштабы речевых сигналов, а возможно незначительное изменение средних масштабов и более свободное изменение мелких масштабов. Данная концепция выбора масштабов называется теорией кратномасштабного анализа и базируется на теории функциональных пространств².

Таким образом, можно решить поставленную задачу в форме вейвлет-преобразования речевых сигналов с последующим прореживанием «мелких» масштабов. Освободившуюся полосу предлагается использовать для передачи вспомогательных сигналов.

Однако для реализации данной задачи необходимо определить, какая часть масштабов сигнала потенциально является свободной и могла бы быть использована для передачи служебной (тайной) информации без ухудшения качества речи. Теоретически решить проблему невозможно, поэтому предлагается путь экспериментальных исследований и анализа данных, полученных в ходе опыта. Кроме того, сформируем критерии, позволяющие оценить возможные потери качества восприятия речи при исключении части масштабов.

Для решения поставленной выше задачи разработана программа, которая может быть представлена следующим алгоритмом:

- ввод данных (аудио-сигналов);
- секционирование данных;
- применение вейвлет-преобразования к секциям;

¹ Shapiro J.M. Embedded image coding using zerotrees of wavelet coefficients. // IEEE Trans. Signal Proc., 41(12), December 1993, с. 3445-3462.

² Devore R.A., Jawerth B., Lucier B.J. Image compression through wavelet transform coding. // IEEE Trans. Info. Theory, 38(2), March 1992, с. 719-746; Sullivan G. Efficient scalar quantization of exponential and laplacian random variables. // IEEE Trans. Info. Theory, 42(5), September 1996, с. 1365-1374.

- оценка мощности речевых сигналов по масштабам;
- процедура выбора порога;
- процедура обнуления масштабов (исключение масштабов, не превышающих порог данного масштаба);
- процедура подсчёта количества обнулённых масштабов для их дальнейшего использования в передаче служебной информации;
- использование обратной операции вейвлет-преобразования с обращением масштабно-временной информации во временную (естественную);
- процедура «склеивания» секций с целью формирования общего временного сигнала;
- предъявление преобразованного сигнала (синтезированной речи) для прослушивания (восприятия) оператором.

В эксперименте участвовали 5 человек без патологии слуховой функции в возрасте от 18 до 25 лет. Прослушивание речи осуществлялось через динамики. Предлагался неискаженный (первичный) отрезок речи, а затем следовал этот же отрезок, но уже с искажениями, т.е. после исключения части речевых масштабов. Каждому оператору (испытуемому) предлагалось дать оценку качества воспринимаемого сигнала по следующим показателям: «различие в качестве восприятия речи неощутимо», «имеет место незначительное ухудшение качества восприятия речи», «имеет место ухудшение качества восприятия речи», «существенное ухудшение качества речи с потерей смыслового содержания». Последовательность предлагаемых для оценки аудио сигналов (с целью исключения субъективных факторов) имела случайных характер.

Исходные речевые сигналы (зачитывался художественный текст) представляют собой женский и мужской голоса, незнакомые для операторов.

Цикл прослушивания аудио сигналов длился 30 мин. В цикле фрагменты нормальной и искажённой речи, составлявшие по времени 25 сек. каждый, предъявлялись в случайном порядке, что обеспечивало реализацию метода вынужденного выбора из двух.

В эксперименте частота дискретизации речевого сигнала f_d при 16-битной звуковой карте составляла 11025 Гц. В качестве вейвлет-преобразования применялось вейвлет-преобразование Хаара. С целью согласования уровней шумов речи, имеющих, как правило, спектральную плотность порядка $1/f^2$, при проведении процедуры представления временного сигнала в масштабно-временной форме (вейвлет-преобразование), увеличивалась амплитуда высокочастотных масшта-

бов. Или, с увеличением масштаба в 2 раза, его амплитуда уменьшалась также в 2 раза.

Процедура принятия решения была следующей:

$$\Psi_p(t, \alpha) = \begin{cases} P(t, \alpha) \geq \beta \cdot P_0(\alpha), & \Psi(t, \alpha) \\ P(t, \alpha) < \beta \cdot P_0(\alpha), & 0 \end{cases}, \quad (1)$$

где $P(t, \alpha)$ - мощность вейвлет-сигнала;

t - время;

α - масштаб;

$P_0(\alpha)$ - средняя мощность по масштабам;

β - коэффициент, задающий порог принятия решения;

$\Psi(t, \alpha)$ - представление речевого сигнала в форме вейвлет-сигнала;

$\Psi_p(t, \alpha)$ - преобразованный вейвлет-сигнал.

В ходе эксперимента коэффициент β позволял регулировать порог принятия решения, а процедура (1), являясь правилом принятия решения, исключала малозначимые сигналы в масштабно-временной плоскости.

На рис. 2, 3 представлены средние распределения мощностей женского и мужского голосов. На оси абсцисс значения масштабов (М) увеличиваются слева направо, т.е. самый крупный масштаб соответствует числу 10. По оси ординат – мощности масштабов (N) представлены в децибелах (дБ). Из рисунков видно, что имеет место существенное различие распределения мощности женского и мужского голосов по масштабам. У женских голосов имеет место подъем мощности для мелких масштабов.

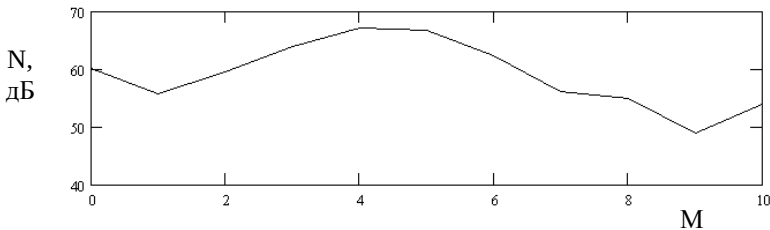


Рис.2. Представление распределения мощности мужского голоса по масштабам.

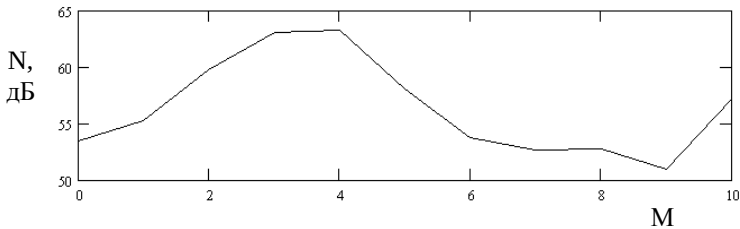


Рис.3. Представление распределения мощности женского голоса по масштабам.

Заметим, что этот признак можно использовать для автоматической классификации мужских и женских голосов. По-видимому, индивидуальные особенности голосов также проявляются при распределении мощности масштабов, и данный факт мог бы быть использован в процессе идентификации личности. Подтверждение этой гипотезы потребовало бы серьезных экспериментальных исследований.

Сформулируем критерий для оценки объема передаваемой служебной информации. Предлагается в качестве критерия принять отношение количества слов, обладающих потенциальной возможностью их использования для передачи служебной информации, к общему количеству передаваемых слов. Слова, которые можно использовать для служебной информации – это слова, соответствующие масштабам с малой энергетикой, т.е. не превышающих порог принятия решения.

В таблице 1. представлены результаты экспериментальных исследований по оценке качества распознаваемой речи и определения объемов аудио сигналов, которые в этом случае можно использовать для передачи служебной (скрытой) информации.

Таблица 1.

Оценки качества расознаваемой речи	Возможные объёмы аудио сигналов для передачи служебной информации, %		Величина, задающая порог принятия решения
	Мужской голос	Женский голос	
Различие в качестве восприятия речи не- ощутимо	3,5	3,2	1/1000
	11	10	1/100
	15	14	1/50
Имеет место незначи- тельное ухудшение ка- чества восприятия речи	32	29	1/10
	43	40	1/5
	60	57	1/2

Имеет место ухудшение качества восприятия речи	75	71	1,0
	83	80	1,5
	87	85	2,0
Существенное ухудшение качества речи с потерей смыслового содержания	90	89	2,5
	92	91	3,0
	94	93	3,5

Как следует из таблицы, при передаче женских и мужских голосов можно использовать 30 % от общего объёма аудио сигнала для служебной информации без существенной потери качества открытой речи.

Вывод: Решена задача возможности передачи служебной информации (до 30 %) вместе со звуковыми сигналами без существенной потери качества и без увеличения пропускной способности акустического канала.

А.Л. Саченко

Гражданско-правовые проблемы защиты интеллектуальной собственности

На рубеже тысячелетий экономические преобразования, захлестнувшие практически всё пространство Восточной Европы в конце 80-х начале 90-х гг. достигли территории России. В свою очередь наше государство, стараясь стать полноправным членом европейского сообщества, открыто признало необходимость строго следовать курсу западной (европейской) модели развития рыночной экономики. Эти обстоятельства вызвали необходимость пересмотреть многие общественные институты и, как следствие этого, изменить нормативную базу с учётом требований новой эпохи.

Наряду с частной собственностью гражданина закон закрепляет за ним и право интеллектуальной собственности. И если в первом случае вот уже на протяжении нескольких лет активно ведётся законодательская работа, то в последнем имеется ряд некоторых упущений. Это объясняется хотя бы тем, что сам термин «интеллектуальная собственность» был введён в обращение в начале 90-х годов, а с принятием Конституции 1993 года получил окончательное правовое закрепление. Тем самым само понятие «интеллектуальная собственность» является практически новым для отечественной юриспруденции.

Сегодня с расцветом в нашей стране товарно-денежных отношений общеизвестным стал тот факт, что материально воплощённые результаты интеллектуальной деятельности человека, как правило, включаются в сферу товарного обращения. Это позволяет сделать вывод о том, что объекты творческой деятельности человека носят коммерческий характер. Соответственно, с развитием рынка результаты интеллектуальной деятельности по своей сути являются товаром, реализуемым в ходе предпринимательской деятельности.

В последнее время особое значение в системе права интеллектуальной собственности придаётся защите авторских и смежных прав. Одной из причин этого является огромный уровень пиратства в сфере авторского права. Так, по данным Ассоциации производителей компьютерного обеспечения уровень только компьютерного пиратства в России составляет около 94 %, в отличие от Германии, где уровень пиратства в данной сфере составляет 50 %, а в США – 35 %.¹ В этом случае не приводятся данные о пиратстве в сфере аудио- и видео- промышленности, хотя это более распространено. Наряду с этим выделение такой отрасли, как коммерческое право, которое рассматривает результаты творческой деятельности в качестве объекта права, из гражданско-правовых наук ставит данный вопрос довольно остро. Развитие института защиты авторских и смежных прав связано с большим влиянием на экономическую ситуацию в нашей стране. Так, российский бюджет в связи с незаконным характером деятельности только продавцов программ ЭВМ недополучает сумму, эквивалентную 85 млн. долларов США. Всё это происходит на фоне того, что существующее гражданское законодательство (Гражданский кодекс РФ, закон РФ от 9 июля 1993 г. «Об авторском праве и смежных правах») содержит большой перечень форм и способов защиты авторских и смежных прав. В сравнении с нормами, которые ранее действовали на территории России в эпоху построения социалистического общества, современные гражданско-правовые нормы в области интеллектуальной собственности направлены, прежде всего, на поддержание индивидуальных качеств субъекта права. Это выражается в том, что в советскую эпоху авторское право закреплялось за государством. Действующие на тот момент правовые рамки создавали условия, когда автор произведения науки, литературы и искусства мог использовать свое произведение, хотя и по своему усмотрению, но только через соответствующую социалистическую организацию. Изобретения, как важнейший по экономической значимости объект интеллектуальной собственности,

¹ «Эксперт» 1996 г. №17, с. 19; «Финансовые известия» 14.05.96.

охранялось только авторским свидетельством, призванным всецело обеспечить исключительное право государства на использование изобретений. Практически отрицался товарный характер результатов духовного производства, за исключением определённой части практических знаний, которые имели потребительскую стоимость, но в основном, только лишь для отдельного конкретного потребителя. По сути, советское законодательство не разграничивало понятия «авторского» и «патентного» права. Таким образом, только государство регулировало имущественные и неимущественные отношения автора. Соответственно, посягательство на права автора рассматривалось, как посягательство на интересы государства, что незамедлительно влекло санкции по отношению к нарушителю авторских прав. Анализируя это, можно сделать вывод о том, что, с одной стороны, в эпоху социализма автор был защищён от неправомерного посягательства на его интересы государством, но, с другой стороны, именно государство создавало массу препятствий автору для осуществления его имущественных интересов.

В настоящее время государство предоставило широкое правовое пространство для осуществления тех или иных интересов автора. Современное гражданское законодательство в области защиты авторских и смежных прав призвано защитить имущественные интересы автора. Так, отличительной чертой новой эпохи является то, что законодательство в области авторского права направлено на защиту частных интересов личности, в нашем случае автора. Но это, наряду с общими социальными причинами влечёт и негативные последствия. Автор, его имущественные и неимущественные интересы остаются один на один с физическим или юридическим лицом, не выполняющим требований, установленных действующим авторским законодательством. Как следствие этого очевиден рост количества нарушений авторских и смежных прав. Объясняется это низким правосознанием граждан, представление которых о данных правах складывается, главным образом, из проведения широко разрекламированных акций по борьбе с видео- и аудиопиратством; неосведомлённостью авторов о своих правах, а также злоупотреблением юридическими лицами законодательством об авторских и смежных правах (например: произведениям, созданным в служебном порядке, присваивается авторство людей, хотя и непричастных к созданию данного произведения, но занимающих определённое должностное положение, после чего произведение перестает быть служебным, и свободно участвует в гражданском обороте). Вследствие этого затрудняется реализация возможностей, заложенных в нормах права. Растёт число частных издательских, звукозаписываю-

щих фирм, средств массовой информации, которые в большинстве случаев пренебрегают существующими нормами права в области интеллектуальной собственности. Торговля пиратской аудио- и видеопродукцией является отличительной чертой современного рынка.

Очевидными являются некоторые неточности, имеющие место в различных нормативно-правовых актах. Так, в конституции РФ понятие «собственность» в её имущественном значении и «интеллектуальная собственность», как результат свободной творческой деятельности отнесены к разным статьям (ч. 1 ст. 35 и ч. 1 ст. 44 Конституции), а правовая формула «владения, пользования и распоряжения» отнесена только к имущественным правам (ч. 2 ст. 35). С принятием первой части Гражданского Кодекса РФ (от 21.10.1994) противоречия, заложенные законом о собственности, были в значительной степени устранены. Так, в соответствии со ст. 138 ГК «интеллектуальная собственность» определена как самостоятельный объект гражданских прав и установлен достаточно жёсткий режим её защиты. В ней говорится, что в случаях и в порядке, установленных настоящим Кодексом и другими законами признаётся исключительное право (интеллектуальной собственности) гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица (фирменное наименование, товарный знак, знак обслуживания).

Законодательство предоставляет большой выбор способов защиты авторских и смежных прав. Подобного рода правовые нормы содержатся в ст. 49 Закона об авторском праве и в ст. 12 ГК, причём, перечень способов защиты авторских прав не является исчерпывающим. Такое положение дел не может не порождать ситуации, когда потерпевший затрудняется в выборе конкретного способа защиты и в будущем с развитием законодательства создаст массу вопросов, связанных с выбором способа защиты. Предполагается, что создание нормативно-правового акта, который охватывал бы все аспекты защиты авторских и смежных прав, как и в целом субъективных прав граждан, эффективно отразится в современных условиях. (Об этом свидетельствуют материалы круглого стола по теме «Защита субъективных прав граждан», заседание членов которого проходило на базе Санкт-Петербургского Университета МВД 31 мая 2001 года).

Нельзя отождествлять такие понятия как «право собственности» в имущественном значении и «право интеллектуальной собственности» так как объекты права собственности в имущественном значении и объекты, к примеру, авторского права, имеют различную правовую природу.

Требует улучшения превентивная деятельность органов исполнительной власти в сфере защиты авторских и смежных прав, так как наряду с общими задачами, стоящими перед ними, одной из функций является решение вопросов, связанных с пресечением правонарушений в области авторских прав. В законе об авторском праве за нарушение авторских и смежных прав предполагается участие государственных органов, осуществляющих административную деятельность. Это также порождает ряд проблем. Конфискация контрафактных экземпляров произведений или фонограмм применяется как дополнительный вид наказания и, в случае истечения срока давности, оно применяться не может. Но в свою очередь в законе об авторских и смежных правах в п. 4 ст. 49 сказано, что конфискация контрафактных экземпляров обязательна. Более того, представляется трудным отследить дальнейшее перемещение изъятой продукции.

В нашей стране происходит нарушение авторских прав не только отечественных, но и зарубежных авторов, иностранных организаций, что в целом подрывает авторитет государства. По оценке Международного альянса по интеллектуальной собственности потери американских компаний из-за пиратства в области информационных технологий только за 1993 год, который во многом явился для нашей страны историческим, составили 444 млн. долларов США¹.

Участие России в международных актах, устанавливающих обязательства стран-участников в области охраны интеллектуальной собственности обязывает не только привести существующее законодательство в соответствие с действующими международными соглашениями, но и на практике соблюдать принципы, которые заложены в этих нормативно-правовых актах. Характерен громкий эпизод, связанный с российским программистом Дмитрием Скляровым, обвинённым правительством США в нарушении цифрового авторского права лишь вследствие различия отечественного законодательства в области защиты авторских прав от законодательства ведущих западных стран.

Совершенствование института защиты авторских и смежных прав, как и в целом права интеллектуальной собственности, положительно повлияет на рост отечественной экономики. Так, для примера, доля индустрии авторского права в валовом национальном продукте Великобритании превысила долю автомобилестроения и пищевой промышленности и сравнялась с долей химических и волоконных отраслей. В целом же, индустрия авторского права является наиболее

¹ Интеллектуальная собственность. Законодательство и практика его применения. М., 1997. С. 195.

быстро развивающейся отраслью экономики большинства стран. Для России развитие института защиты авторского права также положительно повлияет на развитие рынка интеллектуальной собственности, что позволит дополнительно привлечь вложение иностранных инвестиций в данную область и улучшит экономическую ситуацию в стране.

О.А. Таратухина

Мультимедиа технологии и интерактивные модели в системе маркетинга

Развитие национального и международного предпринимательства предъявляет требования к повышению роли и социальной значимости коммуникативной политики и бизнес-коммуникаций. Стержнем взаимодействия и общения был, есть, и будет обмен информацией.

Расширение коммуникаций является следствием эволюции средств массовой информации, процесс которой тесно связан как с вербальным способом организации коммуникаций, так и с формированием и ускоренным развитием сети электронных средств обмена информацией, в том числе невербальной. Появление телевидения, компьютеров, электронных сетей значительно усилило роль электронного восприятия и обмена информацией, что послужило началом формирования мультимедиа технологий.

Газеты, журналы и межличностные коммуникации переходят в сферу вспомогательных средств коммуникативной политики. Этому способствует и ускоряющийся темп нововведений в средствах коммуникаций. Ускорение темпов инноваций в средствах коммуникации оказывает влияние на их формы и меняет структуру индивидуальной и общественной деятельности. Одним из значительных, инновационно-технологических успехов последнего десятилетия является рост продуктивности использования возможностей цифровой обработки данных в системе коммуникаций, то есть внедрения мультимедиа технологий.

Мультимедиа технологии - это сложная, многопрофильная совокупность медиа-средств и компьютерных сетей, способов формирования и реализации коммуникативных возможностей в том числе и в процессе предпринимательской деятельности. Они стали основой возникновения интерактивных маркетинговых и коммерческих коммуникаций. Мультимедиа технологии расширяют и переводят на каче-

ственно новый уровень возможности бизнес-коммуникаций, так как они позволяют использовать любой тип представления информации от текстовой до мультимедийной (графической, аудио- и видео-информации). Информация может быть получена и распространена среди, практически, неограниченного числа потребителей, в любых сферах деятельности - науке, образовании, коммерции, маркетинге, логистике, политике, сфере отдыха и т.д. Такие технологии имеют большое значение как для малого и среднего бизнеса, так и для крупного предпринимательства.

Особенно высокая эффективность применения мультимедиа технологии может быть для предприятий, расположенных в неразвитых промышленных регионах, за счёт компенсации недостатка месторасположения и трудностей поиска информации. В качестве главных форм мультимедиа технологий, послуживших переходом от вербальных к невербальным коммуникациям, выступили электронный обмен информацией (ЭОИ) и система Internet.

В предпринимательской деятельности необходимым условием успеха становится оптимизация коммуникаций с деловыми партнерами на основе электронного обмена информацией. Широкое применение при оптимизации внешних и внутренних коммуникаций фирмы находит система EDIFACT (Electronic Data Interchange For Administration, Commerce and Transport) – мировая ратифицированная регулируемая система для электронного обмена информацией в рамках бизнес-коммуникаций, не ограниченных границами отрасли, в сфере администрирования, коммерции и транспорта. Цель EDIFACT состоит в том, чтобы осуществлять деловые безбумажные транзакции с использованием стандартизированной электронной деловой информации. EDIFACT позволяет передавать деловую информацию на протяжении всех звеньев цепочки создания стоимости продукта: от формирования предложения, заказа и снабжения сырьём, полуфабрикатами и конечными продуктами от поставщиков до производства, поставки товара, обслуживания клиентов и внешних инфраструктурных образований (банки, страховые организации, таможни). Широкое использование системы EDIFACT возможно благодаря её стратегическим и оперативным преимуществам.

К стратегическим достоинствам этой системы относят: укрепление связей с клиентами; поддержание имиджа; более тщательный и корректный анализ рынка за относительно короткое время; возможность применения независимо от расположения фирмы; более высокую удовлетворённость потребителей за счёт ускоренной обработки заказов на обслуживание; возможность расширения рыночной доли;

улучшение использования времени на производство; повышение надёжности планирования и сбыта в логических системах; устранение языкового барьера в международных коммуникациях.

К оперативным преимуществам относят: повышение надёжности средств коммуникаций; сокращение ошибок по сравнению с разным набором данных; ускорение процесса передачи информации; сокращение почтовых расходов; упорядочение и ускорение процесса импорта и экспорта товара.

Благодаря электронной коммуникации предприятия могут создавать и усиливать связи с клиентами и покупателями.

Интерактивные коммуникации - это в основном отношения или взаимодействие, базирующиеся на использовании вычислительной техники. В процессе таких коммуникаций пользователь может получить доступ к предложенной информации в любое время, в любом месте, свободно и многократно, на месте (автономно) или из другого места сетевым путём (неавтономно).

Интерактивные коммуникации базируются на цифровых автономных носителях информации, к которым относят дискеты, лазерные диски, терминалы и портативные вычислительные машины. В отличие от личных коммуникаций такое общение предполагает применение компьютеров. Дискеты и лазерные диски – быстро развивающиеся, стандартизированные и легко транспортируемые носители (посредники) коммуникаций. Их можно раздавать выбранной целевой группе при покупке, на ярмарках, выставках или рассылать по почте. Объём хранимой лазерными дисками и информации предоставляет практически полную свободу аудио и визуального оформления коммуникаций в рамках согласованности мощности компьютера и применяемого мультимедиа средства.

Стационарный терминал позволяет пользователю свободно определять практически все параметры своего носителя коммуникаций – техническую оснащённость, оптическое оформление, интерфейс, местоположение, подключение к сети. Терминалы имеют высокий уровень реакции на поставленные пользователем задачи, звуковое и визуальное воспроизведение информации. В качестве пользовательских интерфейсов, наряду с периферийными устройствами, такими, как принтеры, установки для использования магнитных и чипкарт, сканеры, аудио- и видеотелефоны, прежде всего, применяются дисплеи. Для расширения возможностей получения коммерческой и маркетинговой информации терминалы подключают к товарно-экономической системе.

Портативные вычислительные машины как носители коммуни-

каций являются контролируемые системами. Высокие издержки производства портативных ЭВМ дают возможность их применения только в выборочных ситуациях для поддержания коммуникаций.

С помощью интерактивных медиа систем возможен многоступенчатый диалог с пользователем. Однако диалог с интерактивными медиа средствами ограничен по сравнению с межличностными коммуникациями, а смысловое содержание диалога находится в заранее запрограммированных рамках. При интерактивной коммуникации всегда есть и должна быть цель, которая возвратит потребителю вложенные инвестиции (время, внимание и т.д.).

В настоящее время автономные медиа системы всё ещё не находят полностью своего применения в коммуникациях, что вызывается экономическими причинами (издержки производства), психологическим воздействием, появлением конкурирующих медиа средств. В перспективе интерактивные автономные носители коммуникаций найдут более широкое поле применения и займут не последнее место среди различных форм рыночных коммуникаций.

Существенно изменяют характер коммуникации и процесса взаимодействия между предприятиями и клиентами, между различными субъектами системы маркетинга неавтономные носители и средства коммуникаций. Распространение неавтономных носителей предполагает появление таких медиа систем, которые обладают свойством многоканальной коммуникации в противоположность одноканальным коммуникациям на основе классических медиа систем. Неавтономные носители коммуникаций работают в системе онлайн, например Internet и коммерческие online-службы.

Эффективность коммуникаций благодаря использованию неавтономных носителей достигается за счёт повсеместной интенсификации информационных процессов. Интенсификация информатизации предпринимательской деятельности обеспечивает: возрастание скорости передачи сообщений и ускорение коммуникаций; увеличение пропускной способности каналов коммуникативной сети; ускорение обработки информации и увеличение её объема; совершенствование процессов отображения информации; рост функциональных возможностей оборудования и т.д.

Благодаря интенсификации информационных процессов за единицу времени используется больший объём полезной информации, что приводит к ускорению и повышению эффективности коммуникаций.

Для обеспечения высокой конкурентоспособности и эффективности предпринимательской деятельности предприятиям необходимо применять технологии, которые достаточно полно отражают динамику

современных информационных процессов. Такой технологией, в максимальной мере вобравшей в себя достижения современной науки, является глобальная компьютерная сеть Интернет, которая является первой реализацией опосредованной компьютерами гипермедийной среды (ОКГС). ОКГС отличается от электронной диалоговой информационной системы своей многосторонней коммуникативностью. Компьютерная информационная гипермедиа среда представляет собой динамическую, как правило глобальную, распределённую сеть, которая включает в себя и аппаратное и программное обеспечение. Она позволяет проводить интерактивные процедуры и общение в этой среде. Гипермедиа среда, созданная, компьютерным взаимодействием, становится коммуникативным пространством, обладающим определённым информационным потенциалом, позволяющим осуществление диалога, персональное общение через эту среду коммуникатора и коммуниканта. В этом контексте интерактивность выступает, как способность гипермедиа среды участвовать, осуществлять «живое» общение в диалоге с пользователем и тем самым реализовать свойство гипермедиа среды «виртуальной реальности», т.е. такой реальности, что можно наблюдать, но чего нет на самом деле (виртуальные магазины, офисы, музеи, выставки, биржи и т.д.).

Другой характерной особенностью среды Интернет является наличие гипертекста. Под гипертекстом понимается система информационных объектов, объединённых между собой направленными связями, образующими сеть. Каждый объект связан с информационной панелью экрана, на которой пользователь может ассоциативно выбрать одну из связей. Гипертекст обладает нелинейной сетевой формой организации материала, разделённого на фрагменты, для каждого из которых указан переход к другим фрагментам по определённым типам связей. Гипертекстовая технология ориентирована на обработку информации не вместо человека, а вместе с человеком, то есть становится авторской. Удобство её использования состоит в том, что пользователь сам определяет подход к освоению или созданию материала с учётом своих способностей, знаний и уровня квалификации. Гипертекст содержит не только информацию, но и аппарат её эффективного поиска.

Компьютерным информационным гипермедиа средствам присущи возможности не только создавать условия интерактивности и гипермедиа среды, но и формировать эффект присутствия и возможность передвижения (навигации) в виртуальном пространстве. Эффект присутствия характеризует процесс общения пользователя с окружающей средой, которая формируется материальной средой, окружающей кли-

ента (помещения, рабочее место и компьютер) и гипермедиа средой, созданной взаимодействием компьютерных систем и их совокупным информационным полем. Эффект присутствия обеспечивает общение коммуниканта с коммуникатором не с помощью гипермедиа среды (как посредника), а с самой гипермедиа средой, которая выступает в качестве «живого» коммуникатора.

Сетевая навигация – это возможность свободного передвижения в виртуальном пространстве компьютерной информационной гипермедиа среды с целью поиска и селекции необходимой для клиента информации или контроля коммуникаций. Внедрение гипертекста, мультимедиа технологий, Internet, появление нового менталитета и характеристик гипермедиа среды определило формирование и развитие концепции гипермаркетинга, как методологии и методики решения задач маркетинга в компьютерной информационной гипермедиа среде (Hyper-Marketing Concept).

В.А. Титов, канд. экон. наук, доцент

Обеспечение информационной безопасности финансово-кредитных институтов как важное направление деятельности милиции

Руководством МВД отмечено, что одним из приоритетных направлений борьбы с экономическими преступлениями является банковская и бюджетно-кредитная деятельность. Создание электронно-вычислительной техники, её широкое внедрение в экономическую и управленческую деятельность банков привело к повышению значимости информации и информационных ресурсов.

После многих лет небрежного отношения к защите компьютерных данных в финансовом мире наконец признали всю важность этой проблемы. Особенно, вызывает тревогу факт выявления и развития в России нового вида преступлений, связанных с использованием средств компьютерной техники и информационных технологий. Несмотря на многообразие компьютерных преступлений их можно классифицировать по нескольким категориям. Первая категория преступлений - изъятие средств компьютерной техники, мало отличающееся от обычных видов преступлений. Вторая - перехват информации. Он может быть пассивным, активным, осуществляться через несанкционированные радиопередающие устройства (типа «жучков»). Третья - компьютерное пиратство. На многих рынках за небольшую плату

можно приобрести практически любой «вскрытый» программный продукт. Четвёртая категория преступлений - несанкционированный доступ. Это наиболее распространённый вид компьютерных преступлений. При этом главная проблема расследования преступлений в банковских компьютерных системах заключается в установлении самого факта его совершения. Чтобы с полным основанием утверждать, что хищение с использованием компьютера было совершено, необходимо доказать факт проведения определённых неправомерных действий и факт несанкционированного доступа к средствам компьютерной техники либо попытки её «взлома».

Но нельзя не остановиться ещё на одной проблеме. Компьютерные преступления обладают высокой степенью латентности. И она сохранится до тех пор, пока не будет разработана комплексная программа их предупреждения и борьбы с ними. Нужны и типовые инструкции по работе в нештатных ситуациях для сотрудников организаций, ответственных за информационную безопасность. Имеется потребность в разработке программы подготовки и переподготовки сотрудников оперативных, следственных и экспертно-криминалистических подразделений органов внутренних дел.

Кроме этого можно отметить и необходимость профилактики глобальных компьютерных сетей (например, их ежедневный и круглосуточный мониторинг), участие сотрудников правоохранительных органов в приемке средств защиты в банках и подобных учреждениях.

М.Л. Тихомирова

Актуальные проблемы обеспечения авторских прав в цифровой среде

Законом Российской Федерации от 23.09.92 № 3523-1 «О правовой охране программ для ЭВМ и баз данных» программы для ЭВМ отнесены к объектам авторского права, которое возникает у автора в силу создания программы.

Несмотря на кажущуюся безнаказанность хакерской деятельности ввиду несовершенства отечественного законодательства, в настоящее время уже реально существуют механизмы привлечения к ответственности нарушителей. Основными способами нарушения авторских прав являются: редактирование программ; декомпилирование программы; копирование программного обеспечения.

В российском законодательстве есть положения как допускающие редактирование программы, так и запрещающие его под угрозой наказания.

Так, статья 25 Закона Российской Федерации «Об авторском праве и смежных правах» гласит: «...лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без получения разрешения автора или иного обладателя исключительных прав на использование произведения и без выплаты дополнительного вознаграждения внести в программу для ЭВМ или базу данных изменения, осуществляемые исключительно в целях её функционирования на технических средствах пользователя, осуществлять любые действия, связанные с функционированием программы для ЭВМ или базы данных в соответствии с её назначением, а также исправление явных ошибок, если иное не предусмотрено договором с автором».

Пункт 3 этой же статьи вносит оговорку: «... применение положений статьи не должно наносить неоправданного ущерба нормальному использованию программы для ЭВМ или базы данных и не должно ущемлять необоснованным образом законные интересы автора или иного обладателя исключительных прав на программу для ЭВМ или базу данных».

Положения вышеуказанной статьи продублированы в Законе РФ «О правовой охране программ для электронных вычислительных машин и баз данных». Кроме того, ст. 15 этого закона предоставляет законному владельцу программы право «осуществлять адаптацию программы для ЭВМ или базы данных».

Причём, под «адаптацией» подразумевается внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя», что неизбежно ведет к широкому толкованию положений закона.

В то же время существует противоправное по цели и сути редактирование программы. Статья 273 УК РФ предусматривает ответственность за «внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации».

В такой ситуации создаётся возможность нарушения авторских прав, что может повлечь как уголовно-правовое преследование (в порядке ст. 146 УК РФ), так и привлечение к ответственности в соответствии с гражданским законодательством. Другие возможности нарушения авторского права даёт **декомпилирование** программы.

В соответствии со ст. 25 п. 2 Закона РФ «об авторских и смежных правах» декомпилирование является правомерным, когда «...лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия автора или иного обладателя исключительных прав и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, а также для изучения кодирования и структуры программы, при соблюдении следующих условий:

1) информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

2) указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения возможности к взаимодействию;

3) информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления любого другого действия, нарушающего авторское право.

Таким образом, согласно букве закона, декомпилирование допустимо для обеспечения взаимодействия программ и для изучения структуры и кодирования программы.

Наиболее характерным для России нарушением является незаконное копирование программ – пиратство. Его широкое распространение обусловлено колоссальной разницей в цене между лицензионным продуктом и его пиратской копией.

Вместе с тем, в исключительных случаях Закон допускает копирование программного обеспечения. Так, в соответствии со ст. 25 п. 1 Закона РФ «Об авторском праве и смежных правах», «лицо, правомерно владеющее экземпляром программы для ЭВМ или базы данных, вправе без получения разрешения автора или иного обладателя исключительных прав на использование произведения и без выплаты дополнительного вознаграждения изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретённого экземпляра

в случаях, когда оригинал программы для ЭВМ или базы данных утрачен, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных должна быть уничтожена в случае, если владение экземпляром этой программы для ЭВМ или базы данных перестаёт быть правомерным».

В настоящее время помимо юридических гарантий авторского права уже существуют технические средства защиты. Так, компания Microsoft получила патент на операционную систему для защиты авторских прав в цифровой среде (Digital Rights Management Operating System, DRMOS). Система призвана следить за тем, чтобы пользователи потребляли цифровой контент только с помощью «проверенных» программ¹.

Таким образом, в обозримом будущем защита и обеспечение авторского права в цифровой среде будет комплексная: юридическая и техническая.

В.И. Ходюк

Органы внутренних дел и их общая характеристика

Органы внутренних дел, как и составляющие их элементы, относятся к социальным системам. Понятие система прочно вошло в терминологический арсенал почти всех наук. Это в настоящее время наиболее распространенное понятие. Оно является центральным и в науке управления.

Социальные системы – это системы исключительно большого разнообразия и самой высокой степени сложности, поскольку общество рассматривается как живой, находящийся в постоянном развитии организм (а не как нечто механически сцепленное и допускающее поэтому всякие производные комбинации отдельных общественных элементов), для изучения которого необходим анализ производственных отношений, образующих данную общественную формацию, исследования законов её функционирования и развития.

Социальная система может быть определена как структурированный объект социальной природы, характеризуемый системой отношений и функций. Социальные системы могут характеризоваться также наличием установленных целей, отражающих объективно обусловленные потребности социальных субъектов. Любая из больших

¹ Подробнее см.: www.iOne.ru

социальных систем также образована из совокупности относительно самостоятельных подсистем, функционирующих с единой целью. Здесь находят проявление философское понятие единства и тождества целого и частей. Поэтому по поводу следует заметить, что отдельное не существует иначе, как через связь, которая ведёт к общему. Целое и части не абсолютны, а относительны, могут переходить, превращаться друг в друга. Ни система, ни подсистема не являются всегда только целым или частью, а служат и тем и другим одновременно. В зависимости от того, в какой связи они рассматриваются, «целое становится частью более общего и сложного целого, в которое оно входит, а часть становится целым для тех частей, из которых сама образована»¹.

Наиболее общее и достаточно чёткое определение системы следующее: система есть совокупность элементов, образующих единое целое, и взаимодействующих друг с другом, а также с окружающей средой².

Общество – это сложная реальность. В отличие от управляемых систем (где программу воздействия получают извне), общество есть система, в которой процессы управления и регулирования протекают естественно и обуславливаются органами, факторами, механизмами, внутренне присущими самой системе общества³. Важно, что необходимым условием для неё является наличие не менее двух элементов, определённым образом взаимосвязанных, упорядоченных и взаимодействующих друг с другом, и вследствие этого составляющих единое целое, которое обладает присущими только данной системе признаками. Таким образом, для системы необходимо следующее:

- наличие не менее двух элементов;
- взаимосвязанность этих элементов;
- наличие признаков, присущих только данной системе и отличающих её от других.

Следует различать понятия «признаки системы» и «системные признаки».

Первые даны в определении понятия системы, о котором говорилось выше. Это означает, что перед нами целостная система, а не просто сумма каких-то несвязанных предметов и явлений. Они едины и обязательны для всех систем.

¹ См.: Афанасьев В.Г. Научное управление обществом: Опыт системного исследования. М.: Политиздат, 1968. С. 19.

² См.: Теория управления в сфере правоохранительной деятельности: Учебник. М.: Академия МВД СССР, 1990. С. 24.

³ См.: Пановкин Ю.Л. Организация системы управления органами внутренних дел. М., 1997. С. 3.

По системным признакам отличаются друг от друга механические, биологические и социальные системы.

Качественное своеобразие элементов и специфика их связи обуславливают образование конкретной системы (например, машина или коллектив людей). В первом случае она механическая, во втором – социальная. Каждая из них, обладая признаками системы, отличается одна от другой системными признаками¹.

В социальных системах специфика этих признаков предполагает последовательное применение положений науки управления.

В ней существует принцип иерархии систем. «Сочетание принципа иерархичности управления с принципом обратной связи, – подчеркивает академик А. И. Берг, – придаёт системам управления свойство устойчивости, состоящее в том, что система автоматически находит оптимальные состояния при довольно широком круге изменений внешней обстановки»².

Иерархичность предполагает точное определение компетенции и функций управленческих звеньев. Без этого организованная система не сможет действовать чётко и целенаправленно³.

Социальная система в самом упрощённом виде может быть представлена как объединение или даже простейшая группа людей, которые расположены в определённом порядке, соподчинении. Ей присуще наличие целей объединения, которые обуславливаются объективными закономерностями. Но в одном случае цели могут осознаваться людьми, и тогда последние объединяются ради их достижения, в другом – такого осознания не происходит. Однако цели, объединяющие людей как сознательно, так и стихийно, всегда социальные, т. к. определяются экономическими, политическими классовыми и иными общественными интересами.

Высшим типом социальной системы является общество, занимающее самую высокую ступень иерархической лестнице таких систем.

Государство (подсистема) как форма политической организации общества – уже система второго порядка и по отношению к обществу является его элементом. В свою очередь оно состоит из множества

¹ Г.А. Туманов Орган внутренних дел как система управления: Лекция. М.: ВШ МВД СССР, 1972. С. 4.

² Берг А.И. Кибернетика // «Философская энциклопедия», Т. 2. С. 498.

³ Пановкин Ю.Л. Организация системы управления органами внутренних дел. М., 1977. С. 4.

элементов – подсистем – государственных органов различного назначения и размещающихся по всем ступеням иерархии¹.

Специфической управляемой социальной системой, осуществляющей борьбу с преступностью и охрану общественного порядка, является орган внутренних дел любого назначения и уровня.

Здесь мы объединяем понятием «орган внутренних дел» любое системное образование, имеющееся в рамках единой системы органов внутренних дел страны, в том числе и само Министерство внутренних дел России. Отсюда любой такой орган полностью соответствует всем признакам системного образования.

Во-первых, он всегда состоит из каких-то элементов – структурных подразделений и сотрудников; во-вторых, эти элементы связаны между собой определённым образом, что обусловлено должностной и организационной структурой; в-третьих, каждый орган при наличии многих общих с другими признаков – строго индивидуален.

Таким образом, и МВД, и все его структурные подразделения являются специализированными управляемыми социальными системами.

По отношению к государству МВД России выступает как подсистема, но в то же время само по себе является самостоятельной социальной системой, состоящей из своих элементов: МВД республик, УВД областей. В свою очередь элементами структуры УВД являются и подразделения его аппарата, и их службы на местах, и подчинённые ему территориальные органы, и их структурные подразделения, а также отдельные группы сотрудников.

¹ Социальный менеджмент: Учебник / Под ред. Д.В. Валового. М.: ЗАО «Бизнес школа "Интел-Синтез", Академия труда и социальных отношений», 1999. С. 44-49.

В.И. Ходюк;

В.К. Багирбеков, канд. пед. наук, доцент;

О.А. Кокорева, канд. юрид. наук

Виды несанкционированного доступа к средствам компьютерной техники

Получение несанкционированного доступа к средствам компьютерной техники является одним из видов компьютерных преступлений. К получению несанкционированного доступа относятся следующие действия:

1. «За дураком». Этот способ часто используется преступниками для проникновения в запретные зоны - как производственные помещения, так и электронные системы.

Типичный приём физического проникновения хорошо известен специалистам, занимающимся вопросами совершенствования оперативно-розыскной деятельности. Он заключается в следующем: держа в руках предметы, связанные с работой на компьютерной технике (элементы маскировки), нужно ожидать кого-либо, имеющего санкционированный доступ, возле запертой двери, за которой находится предмет посягательства. Когда появляется законный пользователь, остаётся только войти внутрь вместе с ним или попросить его помочь донести якобы необходимые для работы на компьютере предметы. Этот вариант способа рассчитан на низкую бдительность сотрудников организации и лиц, её охраняющих.

На таком же принципе основан и электронный вариант несанкционированного доступа. В этом случае он используется преступником из числа внутренних пользователей путём подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру (обычно используются так называемые «шнурки» — шлейф, изготовленные кустарным способом, либо внутренняя телефонная проводка) в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, выбранной в качестве предмета посягательства, кратковременно покидает своё рабочее место, оставляя терминал или персональный компьютер в активном режиме.

2. «За хвост». Этот способ съёма информации заключается в следующем. Преступник подключается к линии связи законного пользователя (с использованием средств компьютерной связи) и терпеливо дожидается сигнала, обозначающего конец работы, перехватывает его «на себя», а потом, когда законный пользователь заканчивает активный режим, осуществляет доступ к системе. Этот способ технологиче-

ски можно сравнить с работой двух и более неблокированных телефонных аппаратов, соединённых параллельно и работающих на одном абонентном номере, когда телефон «А» находится в активном режиме, на другом телефоне «Б» поднимается трубка, когда разговор по телефону «А» закончен и трубка положена - продолжается разговор с телефона «Б». Подобными свойствами обладают телефонные аппараты с функцией удержания номера вызываемого абонента. Поэтому нет особого различия в том, что подключается к линии связи - телефон или персональный компьютер.

3. «Компьютерный абордаж». Данный способ совершения компьютерного преступления осуществляется преступником путём случайного подбора (или заранее добытого) абонентного номера компьютерной системы потерпевшей стороны с использованием, например, обычного телефонного аппарата. После успешного соединения с вызываемым абонентом и появления в головном телефоне преступника специфического позывного сигнала, свидетельствующего о наличии модемного входа/выхода на вызываемом абонентном номере, преступником осуществляется механическое подключение собственного модема и персонального компьютера, используемых в качестве орудия совершения преступления, к каналу телефонной связи. После этого преступником производится подбор кода доступа к компьютерной системе жертвы (если таковой вообще имеется) или используется заранее добытый код. Иногда для этих целей преступником используется специально созданная самодельная, либо заводская (в основном, зарубежного производства) программа автоматического поиска пароля, добываемая преступником различными путями. Алгоритм её работы заключается в том, чтобы, используя быстроедействие современных компьютерных устройств, перебирать все возможные варианты комбинаций букв, цифр и специальных символов, имеющихся на стандартной клавиатуре персонального компьютера, и в случае совпадения комбинации символов с оригиналом производить автоматическое соединение указанных абонентов. Самодельная программа автоматического поиска пароля достаточно проста в плане её математической и программной реализации. Иногда преступниками специально похищается носитель машинной информации с уже имеющимся паролем доступа, как это видно из примера, приведённого нами при рассмотрении первой группы способов совершения преступления. После удачной идентификации парольного слова преступник получает доступ к интересующей его компьютерной системе.

Стоит обратить внимание на то, что существует множество программ-«взломщиков», называемых на профессиональном языке

HACKTOOLS (инструмент взлома). Эти программы работают по принципу проси́пи перебора символов, которые возможно ввести через клавиатуру персонального компьютера. Но они становятся малоэффективными в компьютерных системах, обладающих программой-«сторожем» компьютерных портов, ведущей автоматический протокол обращений к компьютерной системе и отключающей абонентов в случае многократного некорректного доступа (набор ложного пароля). Поэтому в последнее время преступниками стал активно использоваться метод «интеллектуального перебора», основанный на подборе предполагаемого пароля, исходя из заранее определённых тематических групп его принадлежности. В этом случае программе-«взломщику» передаются некоторые исходные данные о личности автора пароля, добытые преступником с помощью других способов совершения компьютерного преступления. По оценкам специалистов, это позволяет более чем на десять порядков сократить количество возможных вариантов перебора символов и на столько же - время на подбор пароля. Как показывают многочисленные эксперименты, вручную с использованием метода «интеллектуального перебора» вскрывается 42 % от общего числа паролей, составленных из 8 символов (стандартная величина названия файла). Интересны результаты экспериментов, представленные специалистами в форме таблицы:

Тематические группы паролей	% частоты выбора пароля человеком	% вскрываемости пароля
Имена, фамилии и производные	22,2	54,5
Интересы (хобби, спорт, музыка)	9,5	29,2
Даты рождения, знаки зодиака свои и близких, их комбинации с первой группой	11,8	54,5
Адрес жительства, место рождения	4,7	55,0
Номера телефонов	3,5	66,6
Последовательность клавиш ПК, повтор символа	14,1	72,3
Номера документов (паспорт, пропуск, удостоверение и т.д.)	3,5	100,0
Прочие	30,7	5,7

В ходе проникновения в информационные сети преступники иногда оставляют различные следы, заметив которые подвергшиеся нападению субъекты нападения меняют систему защиты информации. В ответ на это некоторые преступники намеренно сохраняют следы в первом персональном компьютере информационной сети, вводя таким способом в заблуждение сотрудников служб компьютерной безопасности, которые начинают считать, что имеют дело с неопытным любителем-дилетантом. Тем самым теряется бдительность при контроле за другими системами, к которым преступники получают последующий доступ с помощью применения другого способа.

По существу, «компьютерный абордаж» является подготовительной стадией компьютерного преступления.

4. Неспешный выбор. Отличительной особенностью данного способа совершения преступления является то, что преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в её защите. Однажды обнаружив их, он может не спеша исследовать содержащуюся в системе информацию, скопировать её на свой физический носитель и, возвращаясь к ней много раз, выбрать наиболее оптимальный предмет посягательства. Обычно такой способ используется преступником в отношении тех, кто не уделяют должного внимания регламенту проверки своей системы, предусмотренному методикой защиты компьютерной системы.

5. «Брешь». В отличие от «неспешного выбора», когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляется их конкретизация: определяются участки, имеющие ошибку (ошибки) или неудачную логику программного строения. Выявленные таким образом «бреши» могут использоваться преступником многократно, пока не будут обнаружены. Последнее возможно лишь высококвалифицированным программистом или лицом, непосредственно разработавшим данную программу.

Появление этого способа обусловлено тем, что программисты иногда допускают ошибки при разработке программных средств, которые не всегда удается обнаружить в процессе отладки программного продукта. Например, методика качественного программирования предполагает: когда программа X требует использования программы Y - должна выдаваться только информация, необходимая для вызова Y, а не она сама. Для этих целей применяются программы группировки данных. Составление последних является делом довольно скучным и утомительным, поэтому программисты иногда сознательно нарушают методику программирования и делают различные упрощения, указы-

вая, например, индекс места нахождения нужных данных, в рамках более общего списка команд программы. Именно это и создает возможности для последующего нахождения подобных «брешей».

Уязвимые места иногда могут быть обнаружены преступником не только в программно-логических, но и в электронных цепях. Например, не все комбинации букв используются для команд, указанных в руководстве по эксплуатации компьютера. Некоторые такие сочетания могут приводить и к появлению электронных «брешей» по аналогии с «нулевым» абонентом телефонной сети: случайный незарегистрированный абонентный номер, созданный посредством нарушения логики связи в электрических цепях коммутирующих устройств автоматической телефонной станции (АТС).

Все эти небрежности, ошибки, слабости в логике приводят к появлению «брешей». Иногда программисты намеренно делают их для последующего использования в различных целях, в том числе и с целью подготовки совершения преступления.

5.1 «Люк». Данный способ является логическим продолжением предыдущего. В этом случае в найденной «бреши» программа «разрывается» и туда дополнительно преступник вводит одну или несколько команд. Такой «люк» «открывается» по мере необходимости, а включенные команды автоматически выполняются. Данный приём очень часто используется проектантами программных средств и работниками организаций, занимающихся профилактикой и ремонтом компьютерных систем с целью автоматизации рутинной работы. Реже - лицами, самостоятельно обнаружившими «бреши».

При совершении компьютерного преступления данным способом, следует обратить внимание на то, что при этом всегда преступником осуществляется преднамеренная модификация (изменение) определённых средств компьютерной техники.

6. «Маскарад». Данный способ состоит в том, что преступник проникает в компьютерную систему, выдавая себя за законного пользователя. Системы защиты средств компьютерной техники, которые не обладают функциями аутентичной идентификации пользователя (например, по биометрическим параметрам: отпечаткам пальцев, рисунку сетчатки глаза, голосу и т. п.), оказываются незащищёнными от этого способа. Самый простейший путь к проникновению в такие системы - получить коды и другие идентифицирующие шифры законных пользователей. Это можно сделать посредством приобретения списка пользователей со всей необходимой информацией путём подкупа, коррумпирования, вымогательства или иных противоправных деяний в отношении лиц, имеющих доступ к указанному документу; обнаруже-

ния такого документа в организациях, где не налажен должный контроль за их хранением; отбора информации из канала связи и т.д. Так, например, задержанный в декабре 1995 г. сотрудниками московского РУОПа преступник похищал наличные денежные средства из банкоматов банка «Столичный» с использованием обычной электронной кредитной карточки путём подбора цифровой комбинации кода доступа в компьютерную систему управления счетами клиентов банка. Общая сумма хищения составила 400 млн. руб.

Интересен пример и из зарубежной практики: преступник, являющийся законным пользователем компьютерной сети с рабочей станции передал сообщение всем пользователям сервера о том, что его телефонный номер якобы изменен. В качестве нового номера был назван номер собственного персонального компьютера преступника, запрограммированный таким образом, чтобы отвечать аналогично серверу. Пользователи, посылавшие вызов, набирали при этом свой личный код, что предусмотрено правилами электронного обмена информацией. Это обстоятельство и было использовано преступником в корыстных целях. Им был получен исчерпывающий список личных кодов пользователей. Затем, с целью сокрытия своих действий, им было послано сообщение о том, что прежний номер сервера восстановлен.

В компьютерных преступлениях способ «маскарад», так же как и способ «за дураком», может выступать не только в электронной, но и в самой обычной физической форме. Чаще всего в этом случае преступники представляются корреспондентами, сотрудниками различных обслуживающих и вышестоящих организаций и получают необходимый им доступ к средствам компьютерной техники (используют метод легендирования).

7. Мистификация. Иногда по аналогии с ошибочными телефонными звонками случается так, что пользователь с терминала или персонального компьютера подключается к чьей-либо системе, будучи абсолютно уверен в том, что он работает с нужным ему абонентом. Этим фактом и пользуется преступник, формируя правдоподобные ответы на запросы владельца информационной системы, к которой произошло фактическое подключение, и поддерживая это заблуждение в течение некоторого периода времени, получая при этом требуемую информацию, например коды доступа или отклик на пароль.

8. «Аварийный». В этом способе преступником используется тот факт, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ (аварийный или контрольный отладчик). Принцип работы данной программы заключается

в том, что она позволяет достаточно быстро обойти все имеющиеся средства защиты информации и компьютерной системы с целью получения аварийного доступа к наиболее ценным данным. Такие программы являются универсальным «ключом» в руках преступника.

9. «Склад без стен». Несанкционированный доступ к компьютерной системе в этом случае осуществляется преступником путём использования системной полочки, в результате которой возникает частичное или полное нарушение нормального режима функционирования систем защиты данных. Например, если нарушается система иерархичного либо категорийного доступа к информации, у преступника появляется возможность получить доступ к той категории информации, в получении которой ему ранее было отказано.

В.А. Шаповал, канд. мед. наук, доцент

Современные психотехнологии и элементы психотерапии в работе преподавателя вуза

В современных условиях гуманизации высшего образования на фоне коренной смены жизненных и общечеловеческих стереотипов, мировоззренческого и нравственного кризиса значительно возрастает роль преподавателя вуза МВД России, расширяется диапазон его психологического и педагогического воздействия на будущего специалиста правоохранительных органов. Сегодня преподавателю уже недостаточно быть только передатчиком знаний и информации, он должен быть и педагогом, и психологом, и психотерапевтом, владеющим и широко использующим современные психологические технологии. От этого во многом зависят его авторитет и успешность профессиональной деятельности.

Педагогический процесс является частным случаем взаимодействия людей, при котором педагог оказывает на слушателей не только обучающее влияние, но и воздействует на них своей личностью, духовностью, эмоциональностью, получая соответствующий отклик, связанный с их индивидуально-личностными особенностями и эмоциональным состоянием в каждый конкретный момент. Такая ситуация называется психотерапевтическим воздействием в широком смысле слова.

С методической точки зрения психотерапевтическая ситуация представляет собой вербальное (словесное) и невербальное воздействие на личность, помогающее в осознании собственных мыслей,

чувств, желаний и способов поведения. В результате этого человек учится понимать и принимать себя, заботиться о себе, строить свой внутренний мир и отношения с окружающими на основе собственного выбора.

Цель обучения - передача знаний, развитие умений и навыков - также достигается посредством определённого воздействия, влияния, без чего невозможно передать и воспринять никакую информацию. Следовательно, психотерапевтическое взаимодействие в широком смысле имеет общечеловеческую сферу распространения, а эффективность образовательного процесса пропорциональна учёту преподавателем закономерностей и основных принципов этого взаимодействия в отношениях с курсантом (слушателем).

В качестве общих факторов психотерапевтического воздействия педагога можно выделить:

- исходное построение отношений в духе сотрудничества, создающих у обучаемых ощущение безопасности и стимулирующее проявление их познавательных и творческих способностей;
- поощрение обучаемых, нуждающихся в помощи, к обсуждению своих проблем с преподавателем, поддержка их в самостоятельном разрешении проблемных ситуаций;
- учёт мотивационных особенностей и стимуляция нереализованных психологических ресурсов обучаемых, расширяющих возможности восприятия и усвоения ими новой информации;
- стратегическая реорганизация личности и оперативная модификация поведения обучаемых на основе обратной связи и устранения дезадаптивных когнитивных, эмоциональных и поведенческих стереотипов;
- выработка новых, более зрелых, конструктивных способов восприятия, реагирования, поведения и других социальных навыков на модели преподавателя;
- использование убеждения и внушения в явном или скрытом виде;
- стимуляция способности каждого обучаемого быть самим собой, а также постоянного стремления к личностному росту и самоактуализации.

По аналогии с задачей психотерапевта задача преподавателя заключается в том, чтобы помочь обучаемому понять изучаемые проблемы настолько глубоко, чтобы они прочно закрепились в его сознании не как формальные или внешние, а как личностно значимые, име-

ющие внутренний смысл и ценность. В этой связи преподавателю вуза МВД России необходимо:

- обладать умением самодиагностики, самоанализа и самопроектирования, избегая таких известных в психотерапии явлений, как «перпенос», «контрперенос» (вариантом которых является неосознанная проекция своих личных проблем на обучаемых и попытка решения этих проблем «за их счёт»);
- быть открытым к инновациям и готовым к переосмыслению своих профессиональных позиций;
- учиться психологическому анализу ситуаций;
- преобразовывать проблемно-конфликтные и кризисные педагогические ситуации в опыт, способствующий профессиональному и личностному росту;
- расширять арсенал альтернативных педагогических решений;
- осваивать психотехники самоуправления, самоконтроля и передовые психолого-педагогические образовательные технологии, непрерывно помня о том, что подготовка слушателя - это перестройка его внутреннего мира, его психики.

Применение элементов психотерапии в образовательном процессе определяется уровнем педагогического мастерства преподавателя, которое можно рассматривать как единство использования научных закономерностей, передового педагогического опыта и как оптимальную технологию обучения. При этом любая технология обучения – это, прежде всего, применение в педагогической практике достижений современной психологии, базирующихся на личностно-деятельностном подходе, создании условий и предпосылок для становления и реализации индивидуальности объекта обучения. Широкий спектр психотехнологий (гипно-суггестия, гештальт, психосинтез, нейролингвистическое программирование, групповые тренинги и других), пришедших из психотерапии в образовательный процесс, помогает разнообразить подходы и совершенствовать методы преподавания в вузе.

В качестве примера можно привести такую современную прикладную психотехнологию с использованием видеотехники, как тренинг личностной диалогичности. Программа данного видеотренинга направлена на развитие психологической способности участников вступать в отношения развивающегося диалога с самим собой, другими людьми, окружающим миром, и позволяет будущему специалисту правоохранительных органов, преподавателю, курсанту или слушателю:

- повысить эффективность своего участия в различных ситуациях взаимодействия с людьми, продуктивнее строить собственное поведение, овладеть технологией разрешения межличностных противоречий и конфликтов;

- расширить диапазон практических умений конструктивного взаимодействия в условиях бесед, споров, дискуссий, собраний, публичных выступлений, переговоров, а также в отношениях «преподаватель – курсант (слушатель)», «преподаватель – учебная группа», «педагог – коллега»;

- выработать умение противостоять манипулятивному поведению других людей;

- лучше ориентироваться в собственном внутреннем мире (состояниях, потребностях, возможностях), открыть доступ к своим ранее не востребуемым ресурсам;

- расширить диапазон средств самовыражения, овладеть стратегиями достижения успеха и способностью создавать развивающую среду.

Таким образом, в педагогическом процессе, как и в психотерапии, происходят взаимодействие и взаимовлияние людей (вербально и невербально) независимо от формального положения участников этих процессов. С точки зрения целей и задач прослеживается их аналогичная направленность на раскрытие творческих способностей человека и совершенствование его возможностей. В случае психотерапии эти изменения в большей степени связаны с личностной перестройкой, а в случае обучения - с интеллектуальной, хотя это различие можно считать весьма условным. Поэтому учёт практически важных моментов психотерапевтического воздействия и использование современных психотехнологий поможет преподавателю повысить эффективность своей профессиональной деятельности и позитивно отразится на качестве профессиональной подготовки будущего специалиста правоохранительных органов России.

В.А. Шаповал, канд. мед. наук, доцент;

А.А. Кабанов канд. юрид. наук, доцент

Психодинамически ориентированный метод оценки психического здоровья и личностного развития обучаемых

Прогрессирующая тенденция роста числа состояний психической дезадаптации, **отклоняющегося поведения** и пограничных психических расстройств, имеющих определённое значение среди причин отчисления курсантов из вузов МВД РФ и увольнения сотрудников из органов внутренних дел, большие материальные потери, связанные с обучением и подготовкой уволенных, а также высокая степень социальной опасности этих лиц в экстремальных условиях служебно-профессиональной деятельности ставят в число важнейших проблему совершенствования первичной психопрофилактики: оценки, прогнозирования и коррекции психического здоровья у кандидатов, курсантов вузов МВД России и сотрудников органов внутренних дел.

Не вызывает сомнения тот факт, что понятие «*психическое здоровье*», отражающее не только отсутствие психических расстройств, но и уровень конструктивно-адаптационных способностей личности и её нервно-психической устойчивости, одновременно обозначает и одно из ведущих профессионально важных качеств сотрудника правоохранительных органов. Диагностика и прогнозирование этого качества является важной задачей системы медико-психологического обеспечения подготовки и профессиональной деятельности сотрудников.

Одной из отличительных особенностей современного состояния дел в области психического здоровья сотрудников ОВД является отмечающийся рост числа пограничных нервно-психических расстройств и донозологических состояний, к которым трудно применить традиционные психиатрические критерии оценки.

Имеющиеся затруднения в успешном решении данной проблемы связаны с неудовлетворённой потребностью ведомственных специалистов психиатров и психологов в современных психодиагностических методах исследования.

Несмотря на достаточно обширный арсенал методик клинической психодиагностики, для решения многих задач в сфере проблем психического здоровья сотрудников органов внутренних дел его всё же явно недостаточно.

Традиционно применяемые в целях медико-психологического и профессионально-психологического отбора кандидатов в органах внутренних дел психодиагностические методики во-первых, устарели и остро нуждаются в серьёзной работе по рестандартизации, ревалидации и реадаптации. Эта необходимость связана с происшедшими за последнее десятилетие существенными изменениями как социально-политической, экономической и демографической ситуации в обществе, так и с трансформацией психологии (менталитета) жителей России. Во-вторых, в связи с коммерческим интересом издателей в подавляющем большинстве психодиагностические методики стали широко доступны для «тренировки» потенциальных подэкспертных с целью получения «нужного» результата. И, в-третьих, одной из существенных проблем психодиагностических методов, является их значительная привязанность к строго определённым теоретическим концепциям, что в значительной степени усложняет практическое использование тестовых результатов пользователями разного уровня. Другими словами, результаты тестирования, зачастую содержат весьма ценную информацию, но её непосредственное использование в сильной степени зависит от уровня специальной психологической образованности потребителя, в частности, знанием концепции и владением «языком», терминологией метода. А так как, в конечном счёте, пользователем психодиагностической информации является не профессиональный психолог, а представитель кадрово-воспитательного аппарата и руководства, значительно возрастает возможность неадекватно заниженной или завышенной оценки тестовых результатов в связи неквалифицированной, ложной их интерпретацией.

Таким образом, современный психодиагностический инструмент должен позволять не только получать психологически важную информацию, но и представлять её в форме, удобной для практического использования.

В ракурсе практических задач ведомственных медицинской и психологической служб в качестве такого психодиагностического инструментария может быть рекомендован *психодинамически ориентированный личностный опросник (ПОЛО-2000)*.

ПОЛО – 2000 представляет собой опросниковую систему нового поколения для оценки и прогнозирования психического здоровья и личностного развития.

Система разработана нами на базе русскоязычной версии Я-структурного теста Гюнтера Аммона (Тупицин Ю.Я., Бочаров В.В. и др., 1998) с включением в него недостающих коррекционных и некоторых дополнительных шкал, полученных в ходе многолетних исследова-

дований курсантов вузов МВД РФ с помощью Стандартизованного метода исследования личности (Собчик Л.Н., 1990).

Области применения ПОЛО-2000. Как методическое средство для получения эмпирической информации, отражающей *важнейшие показатели* психического здоровья различных групп населения, система позволяет успешно решать следующие задачи:

- осуществлять экспресс-оценку уровня психического здоровья кандидатов при приёме на учёбу в вузы МВД РФ и на службу в органы внутренних дел, а также при массовых психопрофилактических обследованиях различных контингентов обучаемых и сотрудников;
- выявлять психопатологическую симптоматику, в том числе на раннем доклиническом уровне её проявления;
- осуществлять целостную оценку "Я" - структуры личности в совокупности её конструктивных, деструктивных и дефицитарных аспектов;
- определять ресурсы психики испытуемых, степень оптимальности их целостного психического функционирования и уровень реализации ими своего психического потенциала (Я-идентичности);
- прогнозировать поведение человека в повседневных и экстремальных условиях деятельности;
- проводить мониторинг психического здоровья и личностного развития с качественной и количественной оценкой их динамики, а также оценивать психологическую динамику в процессе лечения, психокоррекции и реабилитации;
- получать количественную оценку уровня психического здоровья (психической адаптации, самореализации) различных коллективов, групп, популяций испытуемых при скрининговых эпидемиологических исследованиях;
- изучать специальные контингенты с различными специфическими задачами (выявление групп риска в плане формирования аддиктивного, асоциального, агрессивного, суицидального, компенсаторного и других видов дезадаптивного поведения);
- осуществлять медико-психологическое сопровождение и обеспечение профессиональной деятельности различных категорий обучаемых и сотрудников органов внутренних дел;
- разрабатывать и реализовывать индивидуальные и адресные психокоррекционные, образовательные, психопрофилактические и реабилитационные программы.

Новизна: впервые в России адаптирована психодинамически ориентированная тестовая система, основанная на измерении *центральных бессознательных Я-функций* личности с помощью созна-

тельного самоотчёта в виде самооценок собственных переживаний и поведенческих проявлений в представленных тестовыми утверждениями ситуациях отношений, содержащих опыт психоаналитически ориентированного наблюдения.

ПОЛО-2000 концептуально базируется на основополагающих понятиях динамической психиатрии Гюнтера Аммона, таких как *гуманструктуральная модель личности, Я-идентичность, центральные бессознательные Я(гуман)-функции* и их *конструктивная, деструктивная и дефицитарная составляющие, спектральный характер психических нарушений, намерстывающее развитие Я* и других.

Уровень психического здоровья при этом определяется как *соотношение конструктивных (адаптационных) и деструктивно-дефицитарных (психопатологически изменённых и недоразвитых) составляющих психической активности индивида*, что даёт возможность целостной оценки структуры личности в совокупности её здоровых и патологически изменённых аспектов.

Методика ПОЛО-2000 представляет собой стандартный перечень из 377 утверждений, отражающих различные аспекты функционирования личности и оцениваемых испытуемым как верные или неверные по отношению к нему.

Психодиагностическая система включает в себя блоки шкал четырех уровней:

1. Базисный уровень, содержащий 25 шкал:

- 3 специальных шкалы для оценки степени выраженности тестовых установок: 1) *неискренности*, 2) *аггравации*, 3) *диссимуляции*;
- 18 основных шкал, объединённых в 6 отдельных блоков, отражающих основные центральные бессознательные «Я»-функции:

- 1) *агрессии*
- 2) *страха (тревоги)*,
- 3) *внешнего «Я-отграничения» (контроля внешних границ «Я»);*
- 4) *внутреннего «Я-отграничения» (контроля внутренних границ «Я»);*
- 5) *нарциссизма (степени целостного принятия себя),*
- 6) *сексуальности.*

Каждый из 6 блоков включает по 3 шкалы, отражающих 1) *конструктивную*, 2) *деструктивную* и 3) *дефицитарную составляющие* данной Я-функции.

4 дополнительных факторообразующих шкалы, отражающих имеющийся или вероятный тип психической дезадаптации испытуемого:

- 1) *психосоматический*;
- 2) *невротический*;
- 3) *психопатоподобный*;
- 4) *резидуально-органический*.

II. 3 шкалы второго уровня являются производными конструктивных, деструктивных и дефицитарных составляющих всех шести гуман-функций):

- 1) *общей конструктивности Я-структуры личности*;
- 2) *общей деструктивности Я-структуры личности*;
- 3) *общей дефицитарности Я-структуры личности*

III. 2 шкалы третьего уровня, являющиеся производными шкал второго уровня):

- 1) *адаптационный потенциал личности*;
- 2) *потенциал психической активности личности*

IV. интегральную шкалу четвёртого уровня (производная шкал второго и третьего уровней): *шкала Я-идентичности или ресурс психического здоровья*.

Образуя своеобразную вершину гипотетической «пирамиды» Я-структурной модели личности с основанием из 18 основных шкал первого уровня, шкала Я-идентичности или ресурса психического здоровья может служить результирующим показателем, доступным для представителей кадрово-воспитательного аппарата и руководства, а также для характеристики любой популяции обследуемых лиц.

При бланковом варианте методики первичные результаты обследования подсчитываются в «сырых» баллах с помощью шаблонных ключей шкал и заносятся в специальный профильный бланк, где переводятся в стандартизованные Т-баллы, по которым вычерчивается *графический профиль (психограмма) Я-структуры личности испытуемого*, аналогичный личностному профилю СМЛЛ.

Среднее время обследования испытуемого составляет от 30 до 50 минут.

Ограничением для применения методики может служить возраст испытуемых (моложе 16 лет и старше 65 лет), *низкая степень понимания* испытуемыми смысла утверждений опросника, а также наличие выраженных *рентных установок* обследуемых. Последние определяются с помощью коррекционных шкал системы и влияют на достоверность полученной психодиагностической информации.

Таким образом, психодинамически ориентированный личностный опросник ПОЛО-2000, как психодиагностический инструментальный нового поколения, может быть рекомендован для оценки психического здоровья и личностного развития сотрудников органов внутрен-

них дел, а также для эффективного решения ряда других практических задач ведомственных медицинской и психологической служб.

Н.В. Ярмоленко, канд. техн. наук;

О.М. Медведева

Анализ функций системы управления процессом обучения

В современной педагогике анализ обучения осуществляется с позиций деятельностного подхода. В дидактике обучение рассматривается как абстрактная система взаимодействия деятельностей обучаемого и обучающего. Функциональная структура обучения описывается как цепь циклов. Минимальный (наименьший) цикл – это объединение воздействия обучающего с соответствующим ему учебным воздействием обучаемого.

При разработке концептуальной модели системы автоматизированного обучения были сформулированы следующие функции обучающей системы по управлению обучением:

1) основная функция обучающей системы как системы управления состоит в разрешении противоречия между необходимостью достижения целей изучения и низкой квалификацией обучаемого, как органа управления в отношении изучаемого объекта;

2) основная функция обучающей системы как системы отображения информации состоит в реализации обучающего воздействия, то есть представление учебного элемента в виде наиболее обеспечивающем его усвоение.

Под учебным элементом понимают явления, предметы окружающего мира, методы и способы их использования в деятельности людей внесённые в программу учебного предмета для их изучения.

В отношении форм и методов представления содержания обучения были сформулированы следующие основные требования:

содержание компьютерного обучения должно представлять иерархическую структуру учебного элемента, на исходном уровне которой находятся учебные элементы, усвоенные обучаемым на предыдущих этапах обучения;

логическая структура учебного элемента должна быть полностью завершённой и обеспечивать формализованный анализ взаимосвязи компонентов внутри учебного элемента;

для отображения внутренней логики учебного элемента и закономерностей его функционирования он должен быть представлен в виде логико-смысловой и функциональной моделей;

для эффективного решения задач учебной деятельности обучаемого необходимо представление учебного элемента в форме адаптивной модели с соблюдением форм представления информации обучаемому.

Эффективность реализации может быть обеспечена, если:

- формализовано представление, хранение и переработка всех типов информации;

- существует полное взаимное соответствие между логико-смысловыми моделями решения задач по управлению данными или манипулированию ими;

- существует полное соответствие между логико-смысловыми моделями и функциональными моделями, обеспечивающими предъявление данного учебного элемента обучаемому.

Оценка действий обучения по решению поставленных перед ним задач является критерием обученности. Данная оценка должна отражать результативные действия обучаемого по достижению поставленной цели.

Необходимость соответствия модели обучения целому ряду функций обучающей системы по управлению обучением определяет её многоцелевое назначение, что значительно усложняет решение задач её проектирования.

Педагогическая наука является слабоформализованной областью человеческих, в основном эмпирических знаний. Она не даёт конкретных рекомендаций по разработке и составу моделей обучаемого, тем более, не имеет конкретных рекомендаций по разработке и составу моделей, способных обеспечить решение задач управления учебной деятельностью в реальном процессе обучения.

Решение задачи разработки модели управления обучением предполагает:

- квантификацию целей использования модели обучения;

- выявление обучающих воздействий;

- разработку частных имитационных моделей;

- верификацию и оценку эффективности разработанных частных моделей;

- разработку структуры модели обучения, обеспечивающей эффективный и санкционированный доступ к хранимой информации;

- верификацию и оценку адекватности системы моделей управления обучением.

Фундаментальная закономерность учебной деятельностью дает основание предполагать, что проявление свойства обучаемости у обучаемого существенно зависит от трудоёмкости усвоения учебного

элемента: чем больше трудоемкость, тем меньше свойство обучаемости и ниже качество усвоения учебного элемента.

Справочный материал

Государственное образовательное учреждение высшего профессионального образования – Санкт-Петербургский университет МВД России

Санкт-Петербургский университет МВД России создан в соответствии с Постановлением Правительства Российской Федерации № 611 от 18 июня 1998 года.

Это уникальное высшее учебное заведение осуществляет подготовку научно-педагогических кадров, руководителей горрайорганов внутренних дел, сотрудников для следственных и оперативных подразделений, воспитательных аппаратов и подразделений психологического обеспечения деятельности органов внутренних дел, Государственной противопожарной службы, финансово-экономических и контрольно-ревизионных подразделений МВД России.

В настоящее время начальником Санкт-Петербургского университета МВД России является Виктор Петрович Сальников. Доктор юридических наук, профессор, академик, известен отечественной и зарубежной научной общественности как основоположник нового научного направления в области правоведения, связанного с теорией правовой культуры и правовой культурологией.

Ежегодно слушателями и курсантами Университета становятся несколько тысяч человек, имеющих среднее, среднее специальное и высшее образование. Обучение более 25 тысяч курсантов и слушателей ведётся на 8 факультетах в Санкт-Петербурге. Территориальные филиалы заочного обучения функционируют в городах Великом Новгороде, Мурманске, Петрозаводске и Пскове.

Подготовка кадров ведётся по 7 основным специальностям. В специализированных группах готовятся также специалисты для ГИБДД МВД России; по раскрытию преступлений в сфере компьютерной информации; с углубленным знанием иностранных языков. На специальном факультете Университета, помимо этого, ведётся подготовка студентов по 18 различным специальностям. В Университете обучаются офицеры, имеющие опыт практической работы, и лица, впервые поступившие на службу в МВД России.

Учебный процесс обеспечивают 45 кафедр. Главным условием качественной подготовки выпускников Университета является научный потенциал вуза. Сегодня в Университете работают 134 доктора наук и более 350 кандидатов наук, свыше 150 профессоров и 270 до-

центов, что позволяет успешно решать задачи по подготовке высококвалифицированных специалистов для органов внутренних дел.

К педагогической деятельности привлечены известные учёные – академики, доктора наук, профессора Санкт-Петербурга. При обучении специалистов в Университете широко используется отечественный и зарубежный опыт подготовки сотрудников правоохранительных органов. Университет посетило более 70 иностранных делегаций из США, Великобритании, Германии, Франции, Швейцарии, Финляндии, Швеции, Португалии, Италии, Дании, Румынии, Китая, Бельгии, Израиля, Монголии. Более 20 российских делегаций выезжали за рубеж в Германию, США, Финляндию, Польшу, Гану, Великобританию, Австрию, Бельгию, Францию, Израиль, Швейцарию, Китай и другие страны. Международное сотрудничество установлено с 22 зарубежными правоохранительными органами и образовательными учебными заведениями.

Международное сотрудничество способствует повышению профессионального мастерства постоянного и переменного состава Университета, который является не только образовательным учреждением, но и мощным научным центром по разработке и исследованию проблем теории и практики деятельности органов внутренних дел.

Научный потенциал и условия для творческой и исследовательской работы позволяют вести качественную подготовку учёных-юристов, педагогов, психологов и инженеров высшей квалификации. Широта научных интересов и высокий профессионализм, большой опыт научно-педагогической деятельности и владение современными методами научных исследований, постоянный поиск наиболее оптимальный путей решения современных проблем позволяют руководству Университета приумножать мощный научно-педагогический потенциал вуза, обеспечивать непрерывность и преемственность образовательного процесса.

Подготовка научно-педагогических и научных кадров в Санкт-Петербургском университете МВД России осуществляется в докторантуре по девяти научным специальностям, в адъюнктуре - по десяти научным специальностям, а также в форме соискательства.

Результаты научных исследований находят своё воплощение в издаваемой университетом научной литературе. Наиболее значительными работами, выпущенными в свет в 1999-2001 гг., являются серии: «Классики русской философии права», «Классики истории и философии права», «Мир культуры, истории и философии», «Мир медицины», «Учебники для вузов. Специальная литература», «Наркомания: социальная опасность», «Наркомания в армии (социологический ана-

лиз)», «Экономическая безопасность Российской Федерации (ч. 1 и ч. 2)», «Национальная безопасность России: конституционное обеспечение» (автор и руководитель проектов В.П. Сальников); монографии: А.В. Горожанин «Кадры органов внутренних дел: современные проблемы обеспечения», Н.И. Хабибулина «Государственная идеология и язык закона», А.Г. Черненко «Общероссийская национальная идеология и государственность», А.И. Числов «Профессионализм и деятельность сотрудников милиции», В.П. Сальников «Муртаза Рахимов: державник или удельный князь», А.И. Каплунов «Применение и использование сотрудниками милиции огнестрельного оружия: теория и практика». Большое внимание уделяется также обеспечению образовательного процесса учебной и методической литературой. В 1998-2001 гг. профессорско-преподавательским составом Университета было подготовлено и издано более 400 учебников и учебно-методических пособий.

Особое внимание уделяется практической реализации результатов научных исследований, воплотившихся в изданиях сборников «Взаимодействие правоохранительных органов и экспертных структур при раскрытии тяжких преступлений» (в 3-х частях), «Проблемы правонарушений несовершеннолетних и пути их решения», «Психолого-педагогическая подготовка сотрудников ОВД», «Теория и практика криминалистического оружиеведения»; книги «Вопросы работы правоохранительных органов по раскрытию и расследованию серийных преступлений против личности и убийств по найму». Большой интерес для специалистов представляют регулярно издаваемые сборники трудов докторантов, адъюнктов и соискателей, аннотированный список диссертационных работ, защищённых в диссертационных советах Университета, информационные бюллетени и выпуски экспресс-информации.

Санкт-Петербургский университет МВД России – это головная научная организация по разработке проблем совершенствования кадровой и воспитательной работы с личным составом органов внутренних дел, которая выполняет функции научного центра в системе МВД России по координации научно-исследовательской деятельности, информации, стандартизации, а также оценке научной новизны исследований, проводимых в этой области.

Университет оказывает существенную помощь правоохранительным органам Санкт-Петербурга в обеспечении охраны общественного порядка, принимал участие в операциях «Вихрь», «Вихрь-антитеррор», а также регулярно привлекается для проведения оперативно-профилактической работы во время культурно-массовых, спор-

тивных и общественно-политических мероприятий. Университет часто посещают руководители международных общественных организаций, занимающихся проблемами правоохранительной деятельности.

Главная идея, вокруг которой сплачивается коллектив Университета и на реализацию которой направлены все усилия, - это создание образцового образовательного и научного заведения, способного подготовить для системы МВД России специалистов XXI века. Вуз осуществляет подготовку, переподготовку и повышение квалификации специалистов для органов внутренних дел, Государственной противопожарной службы, финансово-экономических и контрольно-ревизионных подразделений системы МВД России.

В январе 2001 года завершила работу комплексная комиссия Министерства образования по аттестации и лицензированию государственного образовательного учреждения высшего профессионального образования Санкт-Петербургский университет МВД России. По всем заявленным специальностям Университет получил лицензию и был аттестован на максимально возможный срок для образовательных учреждений университетского типа – 5 лет.

Россия, 198206, Санкт-Петербург, ул. Летчика Пилютова, д.1,
тел.: 144-70-24, факс: 144-70-42, 144-24-39,
dimail: yimc@spb.mvd.ru; e-mail: mail@univermvd.ru
Internet: www.univermvd.ru

Под общей редакцией кандидата юридических наук, доцента
А.А. Кабанова

Правовая информатика

**Материалы выступлений на заседании
17 секции 20 международной конференции «Школьная
информатика и проблемы устойчивого развития» в Санкт-
Петербургском университете МВД России 28 апреля 2002 г.**

Составитель Никулин А.В.

Печатается в авторской редакции

Подписано в печать и свет 4.11.2002 Заказ № 141 Тираж 100 экз.
Объем 9,8 печ. л. Формат 60x84/16 Печать офсетная. Цена договорная.

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Лётчика Пилютова, д. 1.