МВД России
Санкт-Петербургский университет

Правовая информатика

Материалы выступлений на заседании 20 секции
30 международной конференции
«Школьная информатика и проблемы устойчивого развития»
в Санкт-Петербургском университете МВД России
23 апреля 2011 года

Санкт-Петербург
2011

УДК 34:004
П68

Правовая информатика: Материалы выступлений на заседании 20 секции 30 международной конференции «Школьная информатика и проблемы устойчивого развития» в Санкт-Петербургском университете МВД России. Санкт-Петербург, 23 апреля 2011 г. / Сост. и ред. А.А. Кабанов. – СПб.: СПб ун-т МВД России, 2011. – 100 с.

В сборник включены материалы выступлений на межвузовском заседании 20 секции 30 международной конференции «Школьная информатика и проблемы устойчивого развития». Конференция проходила в Санкт-Петербурге 22-23 апреля 2011 г. под руководством профессора М.Б. Игнатьева, с которым согласовано содержание данного сборника. Секционное заседание состоялось 23 апреля 2011 г. под руководством А.А. Кабанова. Выступления участников приводятся в материалах в алфавитном порядке фамилий авторов.

СОДЕРЖАНИЕ

В.А. Авдяков, канд. техн. наук,
доцент кафедры организации исполнения наказаний
Санкт-Петербургского института повышения квалификации
работников ФСИН России;
Д.С. Хайрусов, канд. юрид. наук,
старший преподаватель кафедры
оперативно-розыскной деятельности
Санкт-Петербургского института повышения квалификации
работников ФСИН России

К вопросу о совершенствовании систем информационной безопасности и защиты информации в учреждениях и органах уголовно-исполнительной системы

Внедрение новых информационных технологий в большинство сфер современного общества оказывает влияние и на органы уголовно-исполнительной системы (УИС). Совершенствуется система управления и информационного обеспечения, возникают новые методы сбора и анализа информации, меняются облик и возможности специальных технических средств и т.п. Более того, информатизация всех подразделений связана не только с переводом системы информации на электронные носители, но и с широким применением территориально распределенных баз данных, вычислительных сетей для обмена оперативной информацией с использованием новых телекоммуникационных средств и систем для развития сотрудничества органов правоохранительных и органов УИС России с аналогичными зарубежными структурами.

Очевидно, что главной проблемой в борьбе с сетевыми преступлениями является транснациональность Интернета. Внутри России специализированные органы достаточно хорошо взаимодействуют со всеми регистраторами и провайдерами. По запросу ведомства они в кратчайшие сроки закрывают неблагонадёжные ресурсы и предоставляют необходимые данные. А вот за пределами страны ситуация совершенно иная.

В настоящее время действия, несущие угрозу для информационных систем УИС можно разделить на *несколько категорий:*

• *действия, осуществляемые авторизованными пользователями:*

- целенаправленная кража данных, замена их на заведомо ложные данные или уничтожение данных на рабочей станции или на сервере;

- повреждение данных пользователем, вызванное неосторожными или халатными действиями;

• *электронные методы воздействия, осуществляемые хакерами:*
- несанкционированное проникновение в компьютерные сети;
- DOS- и DDOS-атаки;
• *компьютерные вирусы;*
• *спам;*
• *естественные угрозы.*

На информационную безопасность могут влиять разнообразные внешние факторы. Так причиной потери данных может стать их неправильное хранение, кража компьютеров и носителей информации, и другие форс-мажорные обстоятельства.

Рассмотрим основные проблемы защиты данных в информационных системах. Построение любой компьютерной сети начинается с установки рабочих станций, следовательно, подсистема информационной безопасности начинается с защиты этих объектов. Здесь возможны:

• средства защиты операционной системы;
• антивирусный пакет;
• дополнительные устройства аутентификации пользователя;
• средства защиты рабочих станций от несанкционированного доступа;
• средства шифрования прикладного уровня.

На базе перечисленных средств защиты информации строится первый уровень подсистем информационной безопасности в автоматизированных системах. На втором этапе развития системы отдельные рабочие станции объединяют в локальные сети, устанавливают выделенные сервера и организуют выход из локальной сети в Интернет. На данном этапе используются средства защиты информации второго уровня – уровня защиты локальной сети:

• средства безопасности сетевых операционных систем;
• средства разграничения доступа к разделяемым ресурсам;
• средства защиты домена локальной сети;
• сервера аутентификации пользователей;
• межсетевые экранные прокси-сервера;
• средства обнаружения атак и уязвимостей защиты локальной сети.

При объединении локальных сетей в глобальную сеть с использованием в качестве коммуникационной среды публичных сетей (в том числе, Интернета) безопасность обмена информацией обеспечивается применением технологии VPN, которая составляет основу третьего уровня информационной безопасности (ИБ).

Рассмотрим более подробно средства защиты, так как разработка таких средств и их усовершенствование есть основная цель сферы

ИБ. Речь идёт не о борьбе с результатом вредоносного воздействия, а в первую очередь о предотвращении его. На фоне возрастающей взаимозависимости в информационных технологиях продолжается рост интенсивности действий злоумышленников и постоянное совершенствование используемых ими методов, атак на информационные системы и сети. В то же время, несмотря на разнообразие технологий, и решений, используемых для защиты от действий злоумышленников, рынок информационной безопасности можно условно разделить на несколько частей: межсетевые экраны, антивирусы, средства криптографии и средства аутентификации, авторизации и администрирования (AAA).

Неотъемлемым элементом защиты сети органа или учреждения УИС от вторжения злоумышленников является межсетевой экран. Предложение на этом рынке представлено десятками компаний, готовых предоставить решения для любых сред: настольных систем, малого и домашнего офиса (SOHO), административных сетей с выходом в Интернет и т.д.

Поэтому для принятия правильного решения о выборе межсетевого экрана необходимо понимание административных потребностей в обеспечении сетевой безопасности и принципов действия этих продуктов.

Межсетевой экран (firewall, брандмауэр) – это комплекс аппаратных и/или программных средств, предназначенный для контроля и фильтрации проходящего через него сетевого трафика в соответствии с заданными правилами. Основной задачей этого класса продуктов является защита компьютерных сетей (или их отдельных узлов) от несанкционированного доступа.

В общем случае, межсетевой экран использует один или несколько наборов правил для проверки сетевых пакетов входящего и/или исходящего трафика. Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая тип протокола, адрес хоста, источник, порт и т.д. Существует два основных способа создания наборов правил: «включающий» и «исключающий». Правила, созданные первым способом, позволяют проходить лишь соответствующему правилам трафику и блокируют все остальное. Правила на основе исключающего способа, напротив, пропускают весь трафик, кроме запрещённого. Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска нежелательного трафика.

Использование межсетевых экранов может быть эффективным при решении следующих задач:

• защита и изоляция приложений, сервисов и устройств во внутренней сети от нежелательного трафика, приходящего из Интернета

(разделение сетей);

• ограничение или запрет доступа к сервисам сети для определённых устройств или пользователей;

• поддержка преобразования сетевых адресов, что позволяет использовать во внутренней сети частные IP-адреса либо автоматически присваиваемые публичные адреса.

Одна из главных тенденций на рынке межсетевых экранов – увеличение функционала и стремление к универсальности. Кроме непосредственного контроля трафика и разделения сетей функционал современных решений включает в себя:

• глубокий анализ пропускаемого трафика (deep packet inspection);

• шифрование трафика;

• организацию удалённого доступа пользователей к ресурсам локальной сети (VPN);

• аутентификацию пользователей.

Современные межсетевые экраны предоставляют возможность построения виртуальных частных сетей, которые позволяют создавать безопасные каналы передачи данных через публичные сети, предотвращая тем самым перехват и искажение передаваемой информации, а также обеспечивая контроль целостности передаваемых данных. При организации VPN-сетей могут применяться различные методы аутентификации, в том числе сертификаты PKI X.509, одноразовые пароли, протоколы RADIUS, TACACS+.

В настоящее время межсетевые экраны всё чаще предлагаются не в виде отдельных решений, а как компоненты более сложных систем защиты. Потребности рынка продуктов для различных предприятий и удаленных офисов послужили стимулом к созданию специализированных аппаратных устройств с функциями межсетевых экранов. Такие устройства, как правило, представляют собой выделенные серверы с предварительно установленным и сконфигурированным на них программным обеспечением межсетевого экрана, виртуальной частной сети и операционной системой.

С появлением технологий беспроводных ЛВС понятие «защищаемого периметра» теряет свое значение. В этой связи наиболее уязвимым местом внутренней сети становятся мобильные рабочие станции. Для защиты от подобного рода угроз производители разрабатывают технологии типа Network Access Protection (Microsoft), Network Admission Control (Cisco), Total Access Protection (Check Point).

В настоящее время на рынке представлено значительное количество межсетевых экранов различной функциональности. Однако при выборе того или иного решения в первую очередь стоит обратить вни-

мание на управление подобной системой. Так или иначе, качество работы межсетевого экрана напрямую зависит от качества установленного системным администратором набора правил. Кроме того, следует понимать, что межсетевой экран – не панацея от всех угроз и его использование эффективно лишь во взаимосвязи с другими продуктами, среди которых самое заметное место занимают антивирусы, которые мы рассмотрим подробнее.

В связи с тем, что подавляющее большинство вредоносных программ распространяется посредством электронной почты, межсетевые экраны оказываются неэффективными. В арсенале решений этого типа нет средств анализа принимаемых почтовых сообщений. Одним из методов, применяемых системными администраторами наряду с использованием антивирусного программного обеспечения, является фильтрация сообщений, содержащих вложения определённых форматов (чаще всего, исполняемые приложения).

Современные антивирусные программы, при всем их разнообразии, используют лишь два принципиально разных метода обнаружения вредоносных программ:

- поиск по сигнатурам;
- эвристический анализ.

Анализируя средства защиты, необходимо упомянуть о криптографической защите. Средства криптографической защиты информации достаточно давно и широко используются в составе популярных сетевых технологий, таких как виртуальные частные сети (VPN) или Secure Shell (SSH). Однако с целью непосредственной защиты личной или служебной информации применение таких решений до сих пор весьма ограниченно. Так, служебная переписка ведётся открыто, шифрование файлов и дисков тоже мало распространено. В то же время шифрование данных – это один из главных и наиболее надёжных способов предотвращения несанкционированного доступа к информации. Далее будут приведены основные сферы применения криптографических средств защиты информации, а также рассмотрены их различные виды.

Самая широкая сфера потенциального применения криптографических средств – разграничение доступа к конфиденциальной информации и/или сокрытие существования такой информации от нелегитимных пользователей. В масштабе сети эта задача достаточно успешно решается средствами AAA. Однако при защите локальных устройств они чаще всего неэффективны. Особенно острой эта проблема становится в связи с увеличением числа мобильных пользователей.

К сожалению, такое качество, как мобильность, преимущества

которой для современных информационных систем сложно переоценить, на практике оказывается ещё и недостатком. Ноутбук, в отличие от стационарного компьютера, легко потерять, он может быть украден или выведен из строя.

Понятно, что вся информация, которая хранится на ноутбуке, заключена на жёстком диске. Извлечь его из ноутбука в спокойной обстановке – дело пяти минут. Именно поэтому следующие средства защиты от несанкционированного доступа будут бесполезны:

- парольная защита BIOS;
- парольная защита операционной системы;
- средства аутентификации, работающие на уровне приложений.

В то же время применение стойких криптографических алгоритмов, таких как DES, AES, ГОСТ 28147-89, RC4 (с длиной ключа не менее 128 бит), RSA – надёжный способ сделать информацию бесполезной для злоумышленника на многие годы. В настоящее время на рынке существует множество компаний, реализующих эти алгоритмы, как в программных продуктах, так и в виде отдельных устройств.

Рассмотрим физические способы обеспечения информационной безопасности.

Физические меры защиты – это разного рода механические, электронные и электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам информационной системы и охраняемой информации. В перечень физических способов защиты информации входят:

- организация пропускного режима;
- организация учёта, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией;
- распределение реквизитов разграничения доступа;
- организация скрытого контроля деятельности пользователей и обслуживающего персонала информационной системы;
- мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях аппаратного и программного обеспечения.

Когда физические и технические способы недоступны, применяются административные меры обеспечения информационной безопасности. Опыт функционирования предприятий со сложной организацией информационной системы показал, что наилучшие результаты в достижении информационной безопасности достигаются при использовании системного подхода.

Приведём один исторический факт. Крупнейший неядерный взрыв и вызванный им пожар, который можно было наблюдать из кос-

моса, случившийся на территории Советского Союза, был вызван специально оставленной ошибкой ЦРУ США в программном обеспечении. Тайная передача технологии, в которой содержались скрытые дефекты. В неё, в частности, входила компьютерная программа, спровоцировавшая взрыв сибирского газопровода в 1982 году. КГБ выявил причину произошедшего инцидента и сразу издал инструкцию, запрещающую в критических государственных технологиях использовать программное обеспечение западного производства без детальной проверки исходного кода.

В заключение надо отметить, что в Концепции развития уголовно-исполнительной системы Российской Федерации до 2020 года заложено совершенствование систем информационной безопасности и защиты информации, создание резервного центра управления сетевыми ресурсами, позволяющего повысить надёжность хранения и защиты информации; дальнейшее развитие сети специальной связи с целью обеспечения информационной безопасности УИС.

Литература

1. Концепция развития уголовно-исполнительной системы Российской Федерации до 2020 года / Утверждена распоряжением Правительства Российской Федерации от 14 октября 2010 г., № 1772-р. http: //fsin.su/document/index.php?ELEMENT_ID=6663&sphrase_id=21515.

2. Новые педагогические и информационные технологии в системе образования: Учеб. пособие / Е.С. Полат, М.Ю. Бухаркина, М.В. Моисеева, А.Е. Петров; под ред. Е.С. Полат. – 4-е изд., стер. – М.: Издательский центр «Академия», 2009. – 272 с.

3. Компьютерные сети. – 3-е изд., исправл. и доп. / Н.В. Максимов, И.И. Попов. – М.: ФОРУМ, 2008. – 448 с.

Г.И. Бончук,
кафедра экономики и менеджмента
СПбУ ГПС МЧС России

Системные угрозы экономической безопасности России

Ряд угроз экономической безопасности России носит эпизодический характер. Они возникают случайно и, как правило, не наносят существенного ущерба. Более опасными являются системные угрозы. Это, прежде всего, угрозы жизненно важным интересам. Без системного противодействия их невозможно выявить и устранить. Для выявления таких угроз требуется провести системный анализ безопасности в целом, экономической безопасности как одного из основных её ком-

понентов, а также характер и виды угроз экономической безопасности в макро- и микроэкономике.

Как известно, безопасностью называется «состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» [1]. Законодателем эта формулировка более 15 лет не менялась и этому есть серьёзные основания. Совершенно справедливо выделены не просто интересы, а именно «жизненно важные». Не все экономические интересы являются жизненно важными. В самом законе под такими интересами понимается «совокупность потребностей, удовлетворение которых надёжно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Критерии выделения таких интересов, как правило, более подробно не обсуждаются [2].

Кроме того, важной представляется последовательность интересов в соответствии с Конституцией: сначала – интересы личности, затем – общества и только в последнюю очередь – государства. Однако уже в законе «О государственной тайне» в статье 6 абз. 4 последовательность субъектов – прямо противоположна: «исходя из баланса жизненно важных интересов государства, общества и граждан». Причём следует иметь в виду, что личность не всегда является гражданином, может быть иностранцем, апатридом, бипатридом или беженцем.

Бурное развитие мировых рынков и вхождение России на эти рынки как полноценного игрока, влечёт за собой ряд проблем, связанных с экономической безопасностью страны [3, с. 352.], в условиях всеобщей интеграции и объединения Европы, создания единой европейской валюты, даёт европейским государствам гарант защиты от экономической экспансии США и Китая. Учитывая, что экономическая глобализация приводит к совместному использованию капиталов, рабочей силы, научно-технических достижений и углеводородных ресурсов, для России актуальность угроз экономической безопасности возрастает в разы [3, с. 354.].

Реализация национальных интересов России возможна только на основе устойчивого развития экономики и разумной интеграции со странами близким нам по социальным, культурным традициям. Поэтому национальные интересы России в этой сфере являются ключевыми. К числу интересов в экономической сфере следует отнести: стабильность финансовой системы, защиту от терроризма и криминализации общества, рациональное использование природных ресурсов, защиту отечественного товаропроизводителя и т.д. [4, с. 48.].

Проблемам обеспечения экономической безопасности на уровне страны посвящено достаточное количество исследований, в которых её

основные элементы складываются из следующих стратегических аспектов: а) способности экономики функционировать в период смены общественно-экономической формации; б) повышения уровня жизни российского народа; в) формирования устойчивости финансово-банковской системы; г) создания условий взаимовыгодной внешнеэкономической деятельности; д) активизация научно-технического прогресса; е) создания экономических и правовых условий, исключающих криминализацию общества; ж) совершенствования законодательной системы, отвечающей интересам государства и народа; з) государственного регулирования, направленного на стабилизацию и развитие экономики страны. Сущность экономической безопасности в основном представляется как определённое состояние экономики и институтов власти, при котором обеспечивается надёжная защита российских интересов, высокий оборонный потенциал и социально направленное развитие страны в любых даже неблагоприятных условиях, рождаемых внутренними и внешними реалиями [5, с. 7.].

Как показывают исследования ряда учёных, занимающихся проблемами именно экономической безопасности предпринимательства (Сенчагова В.К., Одинцова А.А., Торянникова Б.Н., Красковского А.П.), выжить в таких условиях и обеспечить финансовое благополучие смогли в основном те предприятия, в которых уделялось главенствующее внимание экономической безопасности [5, с. 8.]. Известно, что в развитых капиталистических странах предприниматели выделяют на обеспечение экономической безопасности из годового бюджета от 15% до 25% денежных средств [6, с. 28.].

Угрозы стабильности и жизнеспособности предприятия в зависимости от источника возникновения делят на объективные и субъективные. Объективные возникают без участия и помимо воли предприятия или его служащих, независимо от принятых решений и действий руководителей. Например, состояние финансовых и экономических отношений в стране и за рубежом, научные открытия, форс-мажорные обстоятельства и т.д. Их необходимо распознавать и обязательно учитывать в управленческих решениях. Субъективные же угрозы порождены, как правило, умышленными или неумышленными действиями людей, а также различных органов и организаций, включая, к сожалению, нередко государственные, которые по статусу обязаны содействовать экономической безопасности предприятия [5, с. 9.].

Безопасность может определяться как состояние, при котором не угрожает опасность, есть защита от опасности; или как отсутствие опасности: сохранность, надёжность [7, с. 5.].

Что касается важности геополитического фактора в системе

внешних угроз, то одним из современных заблуждений в области безопасности является то, что в политической жизни России продолжают господствовать стереотипы, сложившиеся ещё до Октябрьской революции – понимание национальной безопасности только как государственной безопасности [8, с. 35.].

Новые геополитические ориентиры диктуют необходимость смены приоритетов [8, с. 36.]. Для многих учёных, ведущих работы в области исследования процессов развития глобального кризиса современной цивилизации, этот кризис является в основе своей мировоззренческим [9, с. 3]. Все остальные кризисные явления (политического, экономического, социального и экологического характера) являются лишь следствиями кризиса мировоззрения [10].

По характеру угрозы экономической безопасности подразделяются на внутренние и внешние. Практически все внутренние угрозы носят не потенциальный, а реальный характер. Из внешних угроз к таковым относятся целенаправленные действия преступников, включающие и нарушение функционирования внешних систем. Нарушения технологического характера, а также чрезвычайные происшествия некриминального характера являются потенциальными источниками угроз. Предотвращение и парирование угроз составляет главное содержание экономической безопасности.

К основным внутренним угрозам, как правило, относят: низкий профессиональный уровень руководителей, нарушения трудовой дисциплины, превышение полномочий руководителями, выбор ненадёжных партнеров и инвесторов, отток квалифицированных кадров, низкую компетентность кадров, нарушения режима сохранения коммерческой тайны, аварии, пожары, взрывы; перебои в энерго-, водо- и теплоснабжении, выход из строя компьютерной техники, зависимость ряда руководителей от уголовного мира, существенные упущения как в тактическом, так и в стратегическом планировании.

К внешним угрозам экономической безопасности следует, прежде всего, отнести: неблагоприятное изменение политической ситуации; изменение законодательства, влияющего на условия хозяйственной деятельности; макроэкономические потрясения (экономические кризисы, нарушение производственных связей, инфляция, потеря рынков сырья, материалов, энергоносителей, товаров и т.д.); противоправные действия криминальных структур; использование недобросовестной конкуренции; промышленно-экономический шпионаж; запугивание, шантаж и физическое воздействие на руководителей и членов их семей; хищения материальных средств; недобросовестная конкуренция; заражение компьютерных систем предприятия различного ро-

да вирусами; противозаконные финансовые операции; чрезвычайные ситуации природного и технического характера; несанкционированный доступ конкурентов к конфиденциальной информации; кражи финансовых средств и ценностей; мошенничество; повреждение зданий, помещений.

К другим внешним факторам, влияющим на результаты хозяйственной деятельности относятся: политическая и экономическая обстановка в стране и регионе предпринимательской сферы, наличие местных сырьевых и энергетических ресурсов, развитие транспортных и других коммуникаций, наполняемость рынка, состояние конкурентов, наличие свободных трудовых ресурсов, уровень их профессиональной подготовленности, уровень жизни населения, его платёжеспособность, криминализация экономики и др.

Выше перечислены угрозы, имеющие место в макроэкономике.

Экономическая безопасность предприятия – это постоянно действующая система мероприятий, гарантирующая стабильность функционирования его организационных структур, финансовую устойчивость предприятия, применение прогрессивных научно-технических достижений и социальное развитие независимо от стабильности или неопределённости внешней среды, а также от возникновения проблем во внутренней среде предприятия.

Основной внешней угрозой экономической безопасности мы считаем криминализацию общества. Если рассмотреть противодействие этой угрозе как управленческий процесс, то следует учесть, что управление имеет несколько определений, подразумевающих, прежде всего наличие цели. Как известно, в управлении организацией проблема целеполагания является центральной [11, с. 213.], она определяет и регулирует действия, и является неким алгоритмом поведения, подчиняющим себе все стороны управляющего воздействия. Среди целей управления выделяют стратегические, тактические и оперативные [12]. Стратегической целью противодействия криминализации как угрозы экономической безопасности является достижение такого состояния системы обеспечения экономической безопасности, которое обеспечивало бы соответствие деятельности всех её подсистем и элементов современному их состоянию, интересам личности, общества и государства, а также адекватное реагирование на новые экономические угрозы, связанные с обострением криминальной ситуации в экономической сфере [13, с. 46.].

Реализация целей обеспечения экономической безопасности, закрепляющих приоритеты государства в указанной области, должна осуществляться [14]:

- в контексте общегосударственной политики реформирования российского общества;

- посредством государственной координации деятельности различных институтов, организаций и учреждений, обеспечивающих экономическую безопасность;

- с использованием внутренних и внешних федеральных, региональных и местных ресурсов – организационных, интеллектуальных, информационных, материальных, финансовых и др.

Криминализация не является исключительно ростом преступности, поэтому защита от неё не сводится только к воздействию на преступность и преступников. Исправить ситуацию, переловив всех бандитов и коррупционеров, невозможно. Подобно тому, как В. Радаев [15, с. 38-39.] характеризует неформальную экономику как сектор или совокупность секторов, совокупность отношений и определённую логику действий, можно характеризовать и российский криминал. Лишь ликвидировав названные выше социальные и культурные предпосылки, осознав, что только от нас зависит наша судьба, можно сделать более выгодным некриминальное поведение.

С позиций обеспечения экономической безопасности комплекс превентивных мер должен состоять: во-первых, из доктрины национальной безопасности, включающей определённую идеологию и программу действий; во-вторых из правовой основы, т.е. системы законов, позволяющих защитить интересы общества и его институтов; в-третьих из системы государственных сил и органов, функциональная задача которых состоит в обеспечении безопасности общества; и, в-четвёртых из системы общественной безопасности.

Условием эффективного функционирования такой системы является ответственность органов власти перед обществом, строгое выполнение системой безопасности своих обязанностей, а также ограничение вмешательства государства в дела общества [16, с. 115-116.].

Обычно выделяют две основные группы организационных механизмов обеспечения декриминализации. Первая группа механизмов – это общие инструменты. Она направлена на уменьшение криминогенного потенциала посредством долгосрочного изменения фундаментальных основ общества. Применительно к экономической сфере, эти инструменты должны воздействовать на экономику в целом. По своей сущности, характеру и по целевому назначению эти инструменты обязаны решать более масштабные проблемы.

Часть механизмов направлена непосредственно на обеспечение декриминализации. К таким механизмам относятся специальные механизмы, непосредственно воздействующие на криминальную экономи-

ку через систему специально уполномоченных на это правоохранительных органов. Специальные меры, в отличие от общих мер, предметно ориентированы и направлены на борьбу с отдельными проявлениями криминализации, и используются на оперативно-тактическом уровне противодействия криминализации. К этой группе следует отнести меры, связанные с так называемой карательной практикой. Совершенствование деятельности в этих сферах предполагает повышение эффективности борьбы с конкретными видами преступности, своевременное реагирование на конкретные преступления, обеспечение неотвратимости наказания лиц, совершивших преступное деяние, возмещение ими вреда потерпевшим и обществу. Следовательно, можно утверждать, что специальные меры обладают направленным воздействием именно на процесс криминализации. К специальным инструментам обычно относят уголовно-процессуальные, административно-правовые, технические, непосредственно экономические и др.

При разработке мер декриминализации, прежде всего, следует учитывать условия места и времени, а также обстоятельства, в которых имеет место криминализация. Однако существуют общие принципы, на которых должна базироваться деятельность по декриминализации. Это, во-первых, комплексное программирование и планирование экономической деятельности; иерархическое деление хозяйствующих субъектов с целью обеспечения их экономической безопасности; чёткое и ясное закрепление за субъектами конкретного уровня определённого круга задач в соответствии с их компетенцией [17].

Можно выделить *принципы обеспечения экономической безопасности* в части декриминализации общества.

Принцип *системности*, который предполагает: во-первых, учёт зависимости между всеми элементами программного комплекса (объектно-субъектные отношения, взаимосвязь целей, задач и средств, методов их достижения и др.); во-вторых, иерархию субъектов декриминализации, чёткое разграничение областей компетенции, функций, ответственности; в-третьих, временно́е структурирование, то есть выделение этапов декриминализации; в-четвёртых, комплексность по отношению к мерам, производимым внутри отдельных элементов программы [18].

Принцип *адекватности*, означающий, что программа действий должна соответствовать условиям времени и места реализации (конкретным историческим условиям, внутреннему и международному положению страны, уровню экономического развития и др.), учитывать их специфику. Если говорить о применении этого принципа непосредственно к объекту исследования, то его суть сводится к тому, что ин-

струменты декриминализации должны отвечать современным тенденциям развития криминальных процессов в нашей стране.

Принцип *вариативности* определяет, что система мер декриминализации должна учитывать все возможные направления криминализации, быть гибкой в соответствии с изменениями криминальной и социальной реальности.

Принцип *открытости* предполагает, чтобы программа строилась с учётом общественных интересов, обеспечивала чёткое усвоение декларируемых целей, задач и их одобрение, поддержку гражданами Российской Федерации. Принцип открытости также предполагает двустороннее взаимодействие между основными субъектами, осуществляющими декриминализацию общества, в вопросах разработки и реализации программы.

Принцип *обратной связи*, заключающийся в постоянном мониторинге состояния преступности и контроле за обеспечением экономической безопасности всеми заинтересованными субъектами. Сущность обратной связи заключается в том, что информация (ресурсы) с выхода системы (или входящих в неё подсистем) поступает на вход этой системы (или подсистем, в неё входящих) [19].

Одной из наиболее опасных для коммерческих предприятий внешней угрозой экономической безопасности является корпоративный захват собственности. Консультационный центр «Стратегия защиты» отмечает, что если за 2002 год на российском рынке было совершено сделок по недружественным поглощениям на общую сумму 3 миллиарда долларов, то за 2003 год – на сумму свыше 15,4 миллиардов долларов. Ежегодно только в одной Москве происходит более 300 захватов предприятий [20]. Под корпоративным захватом (недружественным поглощением) понимается установление над компанией или её активом полного контроля (юридического и фактического) вопреки воле менеджмента и собственников этой компании или её актива.

Можно выделить следующие основные технологии реализации проектов по захвату предприятия:

- скупка акций, распределённых среди большого количества собственников, при условии, что ни один из них не имеет значимого пакета;
- блокировка пакетов акций;
- хищение акций.

Захват предприятия путём скупки акций является самым предпочтительным с точки зрения компании-агрессора. В настоящее время такой способ захвата предприятия является довольно редким, так как в подавляющем большинстве случаев контрольные пакеты акций или

близкие к ним, как правило, или скуплены внешним инвестором, или приобретены советом директоров этих компаний.

Блокировка пакетов акций как способ захвата предприятия встречается чаще. Основной недостаток этого способа для компании-агрессора состоит в том, что блокировка акций даёт лишь кратковременный эффект, однако достаточный для того, чтобы подорвать бизнес конкурента. Блокировка пакетов акций позволяет лишить соответствующего акционера права голосования принадлежащими ему акциями, что и представляет собой угрозу экономической безопасности.

Наиболее распространённым способом захвата предприятия является хищение акций. При этом объектом преступных посягательств являются акции, выпущенные в бездокументарной форме, а таких в практике современного хозяйствования подавляющее большинство. Для того чтобы похитить такие акции, достаточно обеспечить их списание с лицевого счёта конкретного акционера и зачислить на лицевой счёт другого акционера. С помощью цепочки последующих сделок похитители оставляют акционеру только возможность предъявления иска регистратору о возмещении причинённых убытков. Однако эффективность такого иска чрезвычайно низка.

Методика защиты от корпоративных захватов, как представляется, должна быть сориентирована на превентивную защиту от недружественных поглощений. Это, в первую очередь, предполагает:

1) построение защищённой корпоративной структуры;

2) мониторинг текущей ситуации;

3) формирование эффективной мотивации менеджмента и ограничение полномочий руководителей предприятия;

4) создание условий, препятствующих массовой скупке акций [21, с. 131.].

Смысл построения защищённой корпоративной структуры состоит в том, чтобы в максимально степени затруднить возможность недружественного поглощения бизнеса.

Обеспечение эффективной экономической безопасности предприятия с помощью мониторинга текущей ситуации достигается за счёт создания собственной службы безопасности, в структуре которой имеется подразделение бизнес-разведки.

Формирование эффективной мотивации менеджмента и ограничение полномочий руководителей предприятия наиболее эффективны в том случае, если потенциальная компания-цель управляется наёмным менеджментом. Собственникам предприятия необходимо сформировать такую систему мотивации своим управляющим, чтобы они были ориентированы на дальнейший рост компании и развитие суще-

ствующего бизнеса. В противном случае сами менеджеры сами могут выступить инициаторами недружественного поглощения [22, с. 59.].

Создание условий, препятствующих массовой скупке акций, также является актуальным с точки зрения превентивной защиты компании-цели от недружественного поглощения. Наиболее распространённой схемой, позволяющей решить эту проблему, является конструкция перекрестного владения акциями с той лишь разницей, что потенциальная компания-цель создает дочернюю структуру – закрытое акционерное общество с преобладающей долей участия в уставном капитале (51% и более). В качестве остальных учредителей компании выступают миноритарные акционеры, которые вносят в качестве вклада в уставный капитал принадлежащие им акции головного предприятия. Таким образом, у дочерней структуры консолидируется контрольный пакет материнской компании. Генеральный директор компании-цели избирается на должность генерального директора дочернего общества. Получается конструкция, гарантирующая не только контроль над материнской компанией, но и полную несменяемость генерального директора, который на общих собраниях акционеров голосует за собственную кандидатуру. Такую конструкцию крайне сложно разрушить законными средствами. Компании-агрессоры, столкнувшись с описанной структурой перекрёстного владения акциями, обычно отступают.

Таким образом, эффективно построенная система экономической безопасности способна защитить от недружественных захватов.

Практически любой исследуемый социальный механизм – это продукт целенаправленной творческой активности отдельных людей, либо их коллективов, либо социума в целом. В этом смысле проявление общественной активности может быть описано понятием «механизм», во-первых, если в исходном моменте выделяется общий волевой акт; во-вторых, если возникающее явление имеет системообразующие признаки; в-третьих, если созданная система обладает устойчивыми, предсказуемыми параметрами функционирования [23, с. 168-196.].

Экономика всегда сопровождается рисками, также представляющими собой угрозу экономической безопасности. Существует много различных точек зрения по вопросу о сущности риска. Риск – это возможная опасность, действие наудачу, в надежде на счастливый исход, с пониманием того, что могут произойти неприятности, наносящие ущерб. Риск в условиях рыночной экономики становится неизбежным. Идти на риск предпринимателя вынуждает неопределённость, непредсказуемость возникающих в процессе хозяйственной деятельности событий. Под неопределённостью обычно понимается неполнота или не-

точность информации об условиях реализации бизнес-плана, невозможность точного прогнозирования (предвидения) изменений в окружающей среде бизнеса, непредсказуемость в действиях конкурентов, партнёров, невозможность предугадать прорывы в научных открытиях и т.д.

Основными причинами неопределённости являются:

- невозможность полного знания хозяйствующего субъекта об окружающем мире;

- случайность возникновения событий, которые могут привести к убыткам или значительной выгоде;

- непредсказуемость рыночной ситуации (динамика цен, платёжеспособный спрос, наполненность рынка товарами-субститутами и комплиментарными товарами, изменение вкусов потребителей и т.д.);

- противодействие фирме со стороны криминальных элементов, конкурентов, конфликты с партнерами по бизнесу, нарушение договорных обязательств, трудовые конфликты и т.д. [24, с. 55-56.]

Добросовестная конкуренция между участниками экономических отношений является одним из основных критериев рыночной экономики [25, с. 75.]. Тем не менее, опыт социально-экономических реформ в России в условиях затянувшегося переходного периода показывает, что конкуренция в нашей стране не является добросовестной и приобретает всё более и более криминальный характер [26, с. 12-28.].

Недобросовестная конкуренция – любые направленные на приобретение преимуществ в осуществлении предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости, и могут причинить или причинили убытки другим хозяйствующим субъектам-конкурентам либо нанести ущерб их деловой репутации [27].

По справедливому мнению В.Е. Перекислова, недостатки российского законодательства в сфере защиты от недобросовестной конкуренции, обусловленные отсутствием гармонизации правовых норм, сосредоточенных в многочисленных законах, регулирующих экономические отношения в различных сферах, не позволяют обеспечить эффективную защиту бизнеса [28, с. 122.].

Таким образом, выделены наиболее актуальные на наш взгляд системные внутренние и внешние угрозы экономической безопасности предприятия. Подчёркнута важность и реальность внутренних угроз, тем не менее, достаточное внимание уделено внешним угрозам. Кроме того, приведён ряд возможных действий по реализации механизма обеспечения экономической безопасности. Как удалось выявить,

именно системные угрозы представляют наиболее опасные из выявленных угроз. Только системное противодействие этим угрозам позволит обеспечить требуемое состояние безопасности.

Литература

1. Ст. 1 закона РФ от 05.03.1992 № 2446-I «О безопасности» // РГ от 06.05.1992 № 103 (с последними изм. от 02.03.2007 № 24 // РГ от 05.03.2007).

2. Патрушев Н.П. Особенности современных вызовов и угроз национальной безопасности России // Журнал российского права, № 7, июль 2007.

3. Шкварок В.М. Экономическая глобализация как угроза экономической безопасности России // Известия Российского государственного педагогического университета им. А.И. Герцена. № 24 (55): Аспирантские тетради: Научный журнал. – СПб.: 2008.

4. Смирнов А.А. Государственная политика обеспечения экономической безопасности. – СПб.: Изд-во СПбГУЭФ, 2002.

5. Субботин В.Н. Теоретические и практические проблемы обеспечения экономической безопасности предприятия // Экономическая безопасность бизнеса: актуальные проблемы правового обеспечения: Материалы межвузовской научно-практической конференции в СПбГИЭУ. Санкт-Петербург, 19 января 2005 г. – СПб.: СПбГИЭУ, 2005.

6. Экономическая безопасность предпринимательской деятельности. Методическое пособие для предпринимателя / Сост. Б.Н. Торянников, А.П. Красковский. – СПб.: ЗАО «Информационное агентство «Кредитреформа». Санкт-Петербург», 2000.

7. Кабанов А.А. Система защиты государственной тайны: Лекция. – СПб., 2003.

8. Алексеев А.Н. Система внутренней и внешней безопасности: Учеб. пособие. – СПб.: СПбВВКУ ВВ МВД России, 1996.

9. Колин К.К. Информационный подход как фундаментальный метод научного познания. – М.: РАЕН, 1998.

10. Современная картина мира. Формирование новой парадигмы. – М., 1997.

11. Щербина В.В. Социальные теории организации: Словарь. – М.: ИНФРА-М, 2000.

12. Терминология менеджмента: Словарь / Сост. А.К. Семенов, В.И. Набоков. – М.: Маркетинг, 2002.

13. Гончаренко Л.П. Управление безопасностью: Учеб. пособие. – М.: КНОРУС, 2005.

14. Белов О.С. Органы Внутренних дел в системе обеспечения

экономической безопасности: организационные и правовые вопросы (По материалам Приволжского Федерального округа). Дис. … канд. юрид. наук. – М., 2004.

15. Радаев В. Неформальная экономика и внеконтрактные отношения в российском бизнесе. Подходы к исследованию неформальной экономики // Неформальная экономика. Россия и мир / Под ред. Т. Шанина. М., 1999.

16. Мисник В.Л. Превенция терроризма как главное направление взаимодействия антитеррористических центров стран-участниц СНГ // Консолидация усилий правоохранительных органов стран СНГ – основа противодействия транснациональной преступности: Сб. материалов третьей международной научно-практич. конф. «О развитии взаимодействия правоохранительных органов государств-участников СНГ в борьбе с преступностью, международным терроризмом и иными проявлениями экстремизма». – Минск: Тэхналойя, 2001.

17. Лобанова О.В. Особенности криминализации современного российского общества: социокультурный анализ: Автореф. дисс. … канд. социол. наук. – М., 2006.

18. Белов О.С. Органы внутренних дел в системе обеспечения экономической безопасности: организационные и правовые вопросы (По материалам Приволжского Федерального округа): Дис. … канд. юрид. наук. – М., 2004.

19. Кнорринг В. И. Теория, практика и искусство управления. Учебник для вузов по специальности «Менеджмент». – М.: НОРМА-ИНФРА, 1999.

20. Зыкова Т. Троянские кони корпораций // РГ от 2411.2004 № 260 (3637).

21. Ионцев М.Г. Корпоративные захваты. – М.: Ось-89, 2003.

22. Осиновский А.Д. Акционер против акционерного общества. – СПб.: Издательство ДНК, 2004.

23. Смелзер Н. Социология / Пер. с англ. – М.: Фенкс, 1994.

24. Грунин О.А. Науки о безопасности и рисках как инновационный фактор современного образования // Экономическая безопасность бизнеса: актуальные проблемы правового обеспечения: Материалы межвузовской научно-практической конференции в СПбГИЭУ. Санкт-Петербург, 19 января 2005 г. – СПб.: СПбГИЭУ, 2005.

25. Жилинский С.Э. Предпринимательское право (правовая основа предпринимательской деятельности): Учебник для вузов / Предисл. В.Ф. Яковлева. – 4-е изд., изм. и доп. – М.: НОРМА ИНФРА М, 2002.

26. Одинцов А.А. Защита предпринимательства (экономическая

и ин-формационная безопасность): Учеб. пособие. – М.: Междунар. отношения, 2003.

27. Закон РСФСР от 22.03.1991 № 948-I «О конкуренции и ограничении монополистической деятельности на товарных рынках» // РГ № 89, 1991 (с посл. изм. от 26.06.2006 № 135-ФЗ // РГ от 27.07.2006 № 162).

28. Перекислов В.Е. Правовая характеристика недобросовестной конкуренции как угрозы экономической безопасности бизнеса // Экономическая безопасность бизнеса: актуальные проблемы правового обеспечения: Материалы межвузовской научно-практической конференции в СПбГИЭУ. Санкт-Петербург, 19 января 2005 г. – СПб.: СПбГИЭУ, 2005.

Г.И. Бончук,
кафедра экономики и менеджмента
СПбУ ГПС МЧС России;
В.А. Кадулин,
кафедра специальных информационных технологий
Московского университета МВД России

Интеграция системы обеспечения комплексной безопасности объекта в систему мониторинга МЧС РФ

Всевозможные нештатные ситуации, угрожающие жизни и здоровью людей, требуют от служб экстренного реагирования предельно быстрых и точных решений и действий.

В условиях обострения террористических проявлений со стороны экстремистских организаций и незаконных вооружённых формирований, промышленные, транспортные, гражданские и другие объекты всё чаще становятся мишенью террористов.

Почти во всех странах мира для решения подобных задач существуют службы оказания помощи населению в чрезвычайных ситуациях (спасательная служба, скорая медицинская помощь, противопожарная служба, полиция и др.). В работе этих служб есть три общих момента:

- скорость реагирования системы (промежуток времени, прошедший с момента получения сигнала о бедствии и до момента начала оказания помощи);
- как правило, комплексный характер требуемой помощи;
- зависимость эффективности действий служб экстренного реагирования от времени поступления, объёма и достоверности информа-

ции, которой с самого начала располагают спасатели.

Цель работы: определение путей интеграции *системы обеспечения комплексной безопасности* (СОКБ) объекта в систему мониторинга МЧС РФ в интересах повышения оперативности реагирования на чрезвычайные ситуации на охраняемых объектах.

Для достижения поставленной цели в работе решаются следующие задачи:

1. Определение путей интеграции инженерных систем и подсистем безопасности объекта.

2. Выбор метода интеграции системы обеспечения комплексной безопасности объекта в государственную систему предупреждения и ликвидации *чрезвычайных ситуаций* (ЧС).

3. Разработка предложений по интеграции системы обеспечения комплексной безопасности объекта в систему мониторинга МЧС РФ.

Анализ чрезвычайных происшествий и катастроф показывает, что основными источниками угроз промышленным и гражданским объектам являются следующие факторы: техногенная среда, природная среда, человеческий фактор.

Совместное воздействие перечисленных факторов может быть чрезвычайно опасным. Террористические акты или другие угрозы, связанные с человеческим фактором, приводящие к техногенным или природным катастрофам влекут огромные потери.

Для обеспечения эффективного противодействия перечисленным источникам угроз и возможным последствиям от их реализации необходима трёхуровневая взаимосвязанная система обеспечения безопасности:

На первом уровне этой системы стоят задачи по обеспечению безопасности объекта.

На втором уровне – обеспечение безопасности района, округа, города.

На третьем (государственном уровне) – обеспечение безопасности объектов всей страны.

Реализация данной системы безопасности осуществляется поэтапно:

1-й этап. Разработка концепции безопасности объекта.

2-й этап. Разработка и внедрение *автоматизированных систем управления жизнеобеспечением и безопасностью* (АСУ ЖБ) объекта.

3-й этап. Интеграция инженерных систем и подсистем безопасности объекта.

4-й этап. Разработка и внедрение системы обеспечения комплексной безопасности объекта.

5-й этап. Интеграция системы обеспечения комплексной безопасности объекта в систему мониторинга безопасности района, города, области, государства.

Основной задачей интеграции СОКБ объекта в систему мониторинга безопасности объектов города является обеспечение оперативного реагирования сил и средств города по недопущению, пресечению и ликвидации последствий нештатных и чрезвычайных ситуаций на объекте.

В настоящее время МЧС России создаёт систему научного мониторинга катастроф. Большое внимание будет уделяться созданию системы научного мониторинга кризисов и катастроф современной России, оценке и прогнозу современных вызовов и угроз, методам их парирования, а также совершенствованию методов анализа и управления рисками катастроф и стихийных бедствий. Современную систему наблюдения и предсказания чрезвычайных ситуаций в ближайшие годы разработает МЧС России.

Требования по интеграции должны предусматривать:

- сбор, обработку и передачу информации о состоянии системы обеспечения комплексной безопасности объекта в центры мониторинга безопасности МЧС района, города, области и другие заинтересованные службы;

- обеспечение передачи этой информации в различных видах и режимах (реального времени, периодических отчётов и по различным запросам);

- организацию каналов связи между объектом и центрами мониторинга безопасности;

- разработку схем оповещения и алгоритмов действий в различных нештатных и чрезвычайных ситуациях;

- обучение и тренировки персонала объекта, отвечающего за безопасность.

Большое внимание должно уделяться созданию системы научного мониторинга кризисов и катастроф современной России, оценке и прогнозу современных вызовов и угроз, методам их парирования, а также совершенствованию методов анализа и управления рисками катастроф и стихийных бедствий. Коллегия МЧС России утвердила приоритетные направления научно-технической политики ведомства на 2008-2010 годы, в числе которых и создание этой системы.

В соответствии с решением коллегии министерства планировалось подготовить проекты положения и программы внедрения новой техники и технологий в системе МЧС России в 2008-2010 годах.

Интеграция должна предусматривать сопряжение инженерных

систем объекта с техническими средствами и подсистемами безопасности. Для этого необходимо использование стандартных протоколов обмена информации, применение специализированных промышленных контроллеров, которые позволяют сопрягать различные функциональные технические подсистемы. Аппаратно-программная или программно-аппаратная интеграция, создание *интегрированных систем безопасности* (ИСБ) объектов позволяет упростить и удешевить, а также значительно повысить эффективность комплексной системы обеспечения безопасности объекта.

Очевидно, что реализация такого подхода позволяет не только в значительной мере повысить безопасность объектов, но и сократить затраты на создание системы обеспечения комплексной безопасности за счёт оптимального сочетания организационных мероприятий и применяемых для их реализации технических средств.

Наибольшее развитие службы общественной безопасности, использующие самые современные технологии, получили в США, Канаде и странах Европейского Союза. В США и Канаде это телекоммуникационные системы общественной безопасности «911», а в странах Европейского Союза — системы «112». Название эти системы получили по единому телефонному номеру выхода на диспетчерские службы – «911» и «112» (единые объединённые диспетчерские системы). Эти системы работают с начала 70-х годов XX века и достаточно хорошо себя зарекомендовали. В частности, в настоящее время систему 911 используют 90 % населения США.

В России работы по созданию единых объединённых дежурно-диспетчерских систем, являющихся определённым аналогом систем «911» и «112», начались сравнительно недавно. В то же время в России уже имеются во многих городах так называемые «базовые системы» единых диспетчерских систем, в которых телефонные обращения обрабатываются пока ещё вручную. Ряд из этих систем использует единые (для данного города) телефонные номера (005, 051, 059 и др.), но, пока нет единого номера для всей территории России.

Единая дежурно-диспетчерская служба (ЕДДС) является элементом органа повседневного управления местного (городского) звена единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций, создается при органе управления *гражданской обороны и чрезвычайных ситуаций* (ГОЧС) города и является центральным звеном в *объединённой системе оперативно-диспетчерского управления* в чрезвычайных ситуациях (ОСОДУ), в состав которой наряду с ЕДДС входят *дежурно-диспетчерские службы* (ДДС) экстренного реагирования («01», «02», «03», «04»), жилищно-коммуналь-

ного хозяйства, наблюдения и контроля за окружающей средой.

Создание ЕДДС не отменяет существующего до её появления в городских ДДС порядка приёма от населения сообщений о происшествиях (по телефонам «01», «02», «03», «04» и другим).

Вместе с тем ЕДДС является вышестоящим органом для всех ДДС города по вопросам сбора, обработки и обмена информацией о чрезвычайных ситуациях, а также координирующим органом по вопросам совместных действий ДДС в чрезвычайных ситуациях.

Основные *задачи* ЕДДС:

- приём от населения и организаций сообщений о любых чрезвычайных происшествиях;

- анализ и оценка достоверности поступившей информации, доведение её до ДДС, в компетенцию которых входит реагирование на принятое сообщение;

- сбор от дежурно-диспетчерских служб, служб контроля и наблюдения (систем мониторинга) за окружающей средой, и распространение между ДДС города информации об угрозе или факте возникновения ЧС;

- обработка и анализ данных о чрезвычайной ситуации, уточнение состава дежурно-диспетчерских служб, привлекаемых для реагирования на чрезвычайную ситуацию, их оповещение о переводе в высшие режимы функционирования городской системы *российской службы чрезвычайных ситуаций* (РСЧС);

- оценка и контроль обстановки, подготовка вариантов управленческих решений по ликвидации чрезвычайной ситуации, принятие необходимых решений;

- представление докладов (донесений) об угрозе или возникновении чрезвычайной ситуации, сложившейся обстановке, возможных вариантах решения и действиях по ликвидации чрезвычайной ситуации вышестоящим органам управления по подчинённости;

- информирование об обстановке, принятых и рекомендуемых мерах дежурно-диспетчерских служб, привлекаемых к ликвидации чрезвычайной ситуации, подчинённых сил постоянной готовности;

- обобщение информации о произошедших чрезвычайных ситуациях (за сутки дежурства), ходе работ по их ликвидации и представление соответствующих докладов по подчинённости.

ЕДДС города функционирует круглосуточно и при этом должна:

- немедленно приступать к экстренным действиям по предотвращению и (или) ликвидации чрезвычайной ситуации после получения необходимых данных;

- самостоятельно принимать решения по защите и спасению

людей (в рамках своих полномочий), если возникшая обстановка не даёт возможности для согласования экстренных действий с вышестоящими органами управления.

В соответствии с ГОСТ Р 22.7.01-99 «Единая дежурно-диспетчерская служба» (введённого в действие с 01 января 2000 года) целью создания ЕДДС является повышение готовности администрации и служб города к реагированию на угрозу или возникновение чрезвычайных ситуаций [2].

ЕДДС несёт ответственность за своевременность принятия необходимых экстренных мер по защите и спасению людей, материальных и культурных ценностей.

Основными *задачами (согласно этому ГОСТ)* ЕДДС являются:

- приём от населения и организаций сообщений о любых чрезвычайных происшествиях, несущих информацию об угрозе или факте возникновения ЧС;

- анализ и оценка достоверности поступившей информации, доведение её до дежурно-диспетчерской службы (ДДС), в компетенцию которых входит реагирование на принятое сообщение;

- сбор от ДДС, служб контроля и наблюдения за окружающей средой (систем мониторинга) и распространение между ДДС города полученной информации об угрозе или факте возникновения ЧС, сложившейся обстановке и действиях сил и средств по ликвидации ЧС;

- обработка и анализ данных о ЧС, определение её масштаба и уточнение состава ДДС, привлекаемых для реагирования на ЧС, их оповещение о переводе в высшие режимы функционирования *объединённой системы оперативно-диспетчерского управления* в чрезвычайных ситуациях (ОСОДУ);

- обобщение, оценка и контроль данных обстановки, принятых мер по ликвидации чрезвычайной ситуации, подготовка и коррекция заранее разработанных и согласованных с городскими службами вариантов управленческих решений по ликвидации ЧС, принятие необходимых решений (в пределах установленных вышестоящими органами полномочий);

- информирование ДДС, привлекаемых к ликвидации ЧС, подчинённых сил постоянной готовности об обстановке, принятых и рекомендуемых мерах;

- и другие.

ГОСТ Р 22.1.12-2005 «Структурированная система мониторинга и управления инженерными системами зданий и сооружений» (введенный в действие с 1 августа 2005 года) предписывает, оборудование объектов социально-бытового, жилого и иного назначения структури-

рованными системами мониторинга и управления инженерными *системами зданий и сооружений* (СМИС), информационно сопряженными с автоматизированными системами дежурно-диспетчерских служб объектов и ЕДДС с целью предупреждения возникновения и ликвидации последствий чрезвычайных ситуаций, в том числе ситуаций, вызванных террористическими актами.

Основой СМИС являются программно-технические средства, осуществляющие мониторинг технологических процессов и процессов обеспечения функционирования объектов.

Передача информации о состоянии объектов осуществляется по каналам связи в режиме реального времени в ДДС для последующей обработки с целью оценки, прогнозирования угроз и принятии мер по ликвидации последствий от их воздействия.

Основной задачей интеграции системы обеспечения комплексной безопасности (СОКБ) объекта в государственную систему предупреждения и ликвидации чрезвычайных ситуаций является обеспечение оперативного реагирования сил и средств города по недопущению, пресечению и ликвидации последствий нештатных и чрезвычайных ситуаций на объекте.

В качестве примера реализации системы мониторинга безопасности технически сложного объекта приведём разработанный по заказу Управления Гражданской Защиты Москвы МЧС РФ программно-аппаратный модуль для системы обнаружения кризисных ситуаций по поведению потока пассажиров для Московского метрополитена [7].

Разработанный программно-аппаратный модуль является составной частью общей системы мониторинга состояния безопасности на объекте. Основным назначением этого модуля является автоматическое формирование тревожного извещения при возникновении нештатной или чрезвычайной ситуации на транспортном объекте на автоматизированном рабочем месте оператора, путём анализа пассажирских потоков [6,7]. Методом контроля является интегральная оценка получаемой видео- и аудио-информации о состоянии потока пассажиров, сравнение её с ранее записной информацией в период штатной ситуации на транспортном объекте и, в случае обнаружения отклонений, формирование тревожного извещения.

В результате анализа способов идентификации нештатных и чрезвычайных ситуаций на станциях метрополитена были разработаны алгоритм работы и структурная схема модуля (рис. 1).

На схеме выделены основные каналы получения информации и последовательность проведения её обработки.

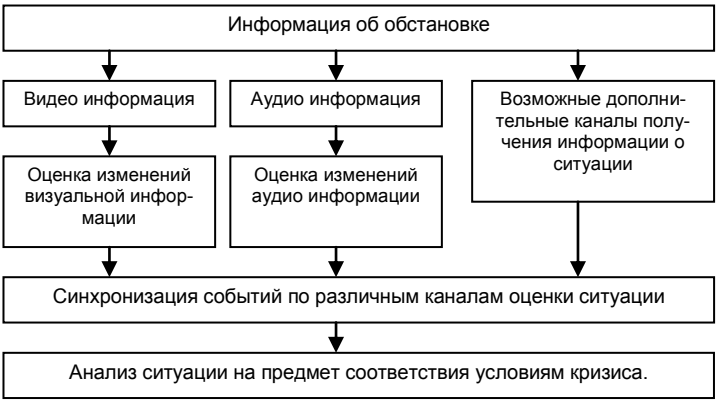

Рис. 1. Алгоритм работы и структурная схема программно-аппаратного модуля определения нештатных и чрезвычайных ситуаций по поведению потока пассажиров

Исходя из требований технического задания и анализа особенностей и условий работы объекта, разработанный программно-аппаратный модуль удовлетворяет следующим прикладным требованиям:

Достаточная скорость работы. Система проводит анализ в темпе, соответствующем скорости ввода информации в систему.

Возможность формирования сигнала тревоги. Система формирует звуковой сигнал и автоматически выводит на экран область видеоизображения, в которой возможно возникает нештатная или чрезвычайная ситуация.

Возможной областью применения подобных систем может служить любой транспортный узел, имеющий плотные пассажирские потоки с определёнными векторами их движения, поддающимися автоматизированной обработке.

В качестве примера интеграции системы обеспечения комплексной безопасности объекта в государственную систему предупреждения и ликвидации чрезвычайных ситуаций целесообразно рассмотреть систему комплексной безопасности Ленинградского железнодорожного вокзала, который расположен рядом с Ярославским и Казанским железнодорожными вокзалами.

Ленинградский вокзал – один из девяти московских железнодорожных вокзалов, пассажирский терминал железнодорожной станции Москва-Пассажирская. Ленинградский железнодорожный вокзал расположен на Комсомольской площади (площадь трёх вокзалов) и явля-

ется самым старым железнодорожным вокзалом Москвы.

С Ленинградского железнодорожного вокзала Москвы отправляются железнодорожные пассажирские поезда, следующие в Санкт-Петербург (две трети всех отправлений), Псков, Великий Новгород, Тверь, Мурманск, Петрозаводск, Хельсинки, Таллинн и по другим железнодорожным направлениям. Помимо пассажирских железнодорожных поездов Ленинградский вокзал обслуживает пригородные электрички, следующие до Крюково (Зеленоград), железнодорожной станции Подсолнечной (Солнечногорск), Клина, Конаково, Бологое.

Между Москвой и Санкт-Петербургом ежедневно курсируют скоростные пассажирские железнодорожные экспрессы «Красная стрела», «Аврора» и «Русская тройка», которые являются лицом и фирменной маркой Ленинградского железнодорожного вокзала Москвы.

Ленинградский вокзал имеет 10 путей, 5 из которых обслуживают поезда дальнего следования, 5 – пригородные поезда. Первоначально вокзал имел дебаркадер, куда заходили поезда. Однако в середине 1970-х годов дебаркадер был ликвидирован, а в 1977 году на его месте был выстроен Большой зал Ленинградского вокзала. Система комплексной безопасности Ленинградского железнодорожного вокзала совместно с Ярославским и Казанским железнодорожными вокзалами требует интеграции в государственную систему предупреждения и ликвидации чрезвычайных ситуаций.

В условиях обострения террористических проявлений со стороны экстремистских организаций и незаконных вооружённых формирований, промышленные, транспортные, гражданские и другие объекты всё чаще становятся мишенью террористов. В этой связи следует особое внимание уделить разработке организационно-технических мероприятий, направленных на борьбу с террористическими актами, и интеграции этих мероприятий в систему обеспечения комплексной безопасности объекта.

Следует отметить, что и концепция и система обеспечения комплексной безопасности объекта должны:

- разрабатываться компетентными организациями с привлечением квалифицированных специалистов, имеющих практический опыт работы в области обеспечения безопасности и владеющих современными научными методами и инструментарием;

- вместе с планом реализации согласовываться в государственных органах и службах, отвечающих за безопасность;

- проходить апробацию в ходе игр и учений по отработке возможных чрезвычайных ситуаций с привлечением руководителей и специалистов всех служб и организаций, отвечающих за безопасность в

городе. Игры и учения должны проводиться как до момента сдачи объекта, так и в процессе его эксплуатации.

В настоящее время разработаны методы и средства *компьютерного имитационного моделирования*, позволяющие проводить указанные игры и учения в учебных классах.

В процессе реализации игр (учений) проводится:

- уяснение последовательности действий служб в условиях нештатной или чрезвычайной ситуации по недопущению (снижению) возможных жертв, материального и иного ущерба;

- отработка организации взаимодействия подразделений и служб при решении первоочередных задач в условиях чрезвычайных ситуаций;

- оценка предлагаемых для защиты объекта технических средств безопасности;

- уяснение необходимости привлечения дополнительных сил и средств в условиях ЧС;

- разработка и корректировка нормативных документов и инструкций по действиям в условиях ЧС.

По результатам проведения игр (учений) проводится корректировка имитационной модели объекта с вариантами обеспечения комплексной безопасности.

Очевидно, что реализация такого подхода позволяет не только в значительной мере повысить безопасность объектов, но и сократить затраты на создание системы обеспечения комплексной безопасности за счёт оптимального сочетания организационных мероприятий и применяемых для их реализации технических средств.

Интеграция системы обеспечения комплексной безопасности объекта в систему мониторинга безопасности района, города, области, государства должна предусматривать:

- сбор, обработку и передачу информации о состоянии системы обеспечения комплексной безопасности объекта в центры мониторинга безопасности МЧС района, города, области и другие заинтересованные службы;

- обеспечение передачи этой информации в различных видах и режимах (реального времени, периодических отчётов и по различным запросам);

- организацию каналов связи между объектом и центрами мониторинга безопасности;

- разработку схем оповещения и алгоритмов действий в различных нештатных и чрезвычайных ситуациях;

- обучение и тренировки персонала объекта, отвечающего за

безопасность.

Основной задачей интеграции СОКБ объекта в систему мониторинга безопасности объектов города является обеспечение оперативного реагирования сил и средств города по недопущению, пресечению и ликвидации последствий нештатных и чрезвычайных ситуаций на объекте.

Предлагаемые методические рекомендации по обеспечению эффективного функционирования интегрированных систем безопасности объектов, содержат различные подходы. Необходимо учитывать условия их создания и эксплуатации на конкретных объектах. Рассмотренный объект – Ленинградский железнодорожный вокзал – и его система обеспечения комплексной безопасности интегрируется в систему мониторинга МЧС РФ совместно с вокзалами Казанским и Ярославским.

Рекомендации по применению автоматизированных систем анализа и принятия управленческих решений предназначены для использования их при создании систем комплексной безопасности на технически сложных и уникальных объектах, а также обеспечения их эффективного функционирования в условиях возникновения и ликвидации чрезвычайных ситуаций. Они должны в полном объёме учитываться при интеграции системы обеспечения комплексной безопасности объекта, в частности Ленинградского железнодорожного вокзала, в государственную систему предупреждения и ликвидации чрезвычайных ситуаций.

Литература

1. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» // РГ от 31.12.2002 (с посл. изм. от 28.09.2010 № 243-ФЗ // РГ от 30.09.2010 № 220).

2. Национальный стандарт ГОСТ 22.1.12-2005 «Безопасность в чрезвычайных ситуациях. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Общие требования». – М.: Стандартинформ, 2005.

3. Федеральный закон от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов» // РГ от 30.07.1997 (с посл. изм. от 27.07.2010 № 227-ФЗ // РГ от 02.08.2010 № 169).

4. РД 50-34.698-9 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

5. СП 11-107-98 «Инженерно-технические мероприятия граж-

данской обороны. Мероприятия по предупреждению чрезвычайных ситуаций».

6. Козьминых С.И. Системный подход к обеспечению информационной безопасности объекта: Учебно-методич. пособие / С.И. Козьминых. – М.: МосУ МВД России, 2005.

7. Козьминых С.И. Методологические основы обеспечения комплексной безопасности объекта, фирмы, предпринимательской деятельности: Монография: в 2-х частях. Ч. 2 / С.И. Козьминых. – М.: МосУ МВД России, 2005.

8. Петренко С.А. Управление информационными рисками. – М.: Компания АйТи; ДМК Пресс, 2004.

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

Некоторые концептуальные вопросы дистанционного обучения

Дистанционное обучение в сфере высшего и среднего специального образования решает ряд важных задач, связанных, прежде всего, с тем, что имеется потребность в обучении у людей, находящихся вдали от высших и средних специальных учебных заведений, и поэтому не имеющих возможности очного обучения. Заочное обучение также затруднено для этих людей вследствие того, что в местах, удалённых от городов, трудно найти необходимую для обучения литературу в актуальном для современных условий состоянии. Значит, первой задачей дистанционного обучения является предоставление возможности обучения лицам, находящимся вдали от образовательных учреждений.

Не менее важным представляется предоставление возможности повышения квалификации лицами, давно закончившими учебные заведения, так как процесс научных исследований и обобщения практического опыта приводит к устареванию знаний и необходимости непрерывного обучения. Эта задача состоит также в предоставлении возможности поддерживать знания в актуальном состоянии для лиц, удалённых от библиотек и коллег, занимающихся исследованиями в интересующей их области. За счёт создания мобильной информационно-образовательной среды, базирующейся на современных информационных и телекоммуникационных технологиях, система дистанционного обучения позволяет повысить уровень доступности образования без потери качества. Процесс дистанционного обучения включает в себя самостоятельное изучение учебно-методических материалов под руководством преподавателя, выполнения контрольных заданий в виде тес-

тов по каждому разделу учебно-практического пособия, вывод итоговой оценки. Кроме того, имеет место и общение между обучаемыми лицами, позволяющее повысить качество обучения.

Определённую пользу в таких ситуациях приносит всё более и более популярный с каждым годом Интернет, как способ обмена информацией, однако сам по себе он лишь предоставляет *возможность* интерактивного общения и передачи информации на расстоянии, а для образовательного процесса необходимы *специальные педагогические средства.* Одним из эффективных средств решения перечисленных проблем является дистанционное обучение. В процессе такого обучения имеется возможность не просто узнать нечто новое, но и убедиться в достаточной полноте и качестве усвоенных знаний, выработке умений и навыков.

Среди средств дистанционного обучения большое значение имеет такая форма предоставления информации, как электронное учебное пособие. В нём содержится и необходимая учебная информация – основные понятия, определения, принципы, методы, правила, приёмы и т.п., а также вопросы для самоконтроля и тесты для проверки усвоенного материала.

Контроль знаний основан на сопоставлении модели знаний обучаемого лица с моделью предметной области по изучаемому предмету. «Привычку к труду молодые люди приобретают, когда они постоянно что-нибудь делают, будет ли это серьёзное дело, или только развлечение»[1]. Тесты должны в достаточной степени охватывать изучаемый предмет, имитировать структуру проверяемого содержания и быть адекватными ему. Они должны отвечать требованиям однозначности и простоты, быть недвусмысленными, не содержать намёков на правильный ответ, использовать наглядные формы предъявления информации, иметь возможность ответа без обращения к справочной литературе. Что касается доступной трудности, то требуется соблюдать соответствие имеющимся знаниям. В частности, в случае, если задание легко выполняется всеми обучаемыми, тесты считаются слишком лёгкими и требуют переработки. Аналогично и в случае, когда задание не может быть выполнено никем из обучаемых лиц. Такие тесты считаются слишком трудными и тоже требуют переработки. Оптимальным считается трудность в пределах 50 %. Кроме того, не рекомендуется использование в тестах задач – головоломок. Назначение тестов – проверка усвоения учебного материала, а не сообразительности.

[1] Коменский Я.А. Великая дидактика. – СПб.: Семья и школа, 1875-1877. – С. 194.

Интересным продолжением идей, реализуемых в дистанционном обучении, является идея так называемого распределённого интеллекта. Один человек не в состоянии знать всё. Коллектив людей, даже самых умных, также ограничен в своих возможностях. А компьютер и тем более система взаимодействующих компьютеров позволяет людям накопить и применять весьма разнородные знания, синтезировать новые обобщённые понятия, решать задачи трансцендентной сложности.

Естественно, знания – это не просто информация. Ведь для понимания букв, появляющихся на экране компьютера, надо иметь элементарную грамотность. В России до революции 1917 года умели читать и писать лишь незначительное количество людей. Сегодня в нашей стране трудно найти людей, не умеющих читать и писать.

Многие дети с увлечением играют в компьютерные игры, лучше взрослых понимают пользу от такого опосредованного общения. Темп обмена информацией с каждым годом возрастает. Поэтому ограничиваться только книжным вариантом передачи знаний от одного человека к другому, от одного поколения к другому поколению – недостаточно. Вопрос – в том, насколько те первые попытки создания электронных учебных пособий, которые предпринимаются нами, соответствуют потребностям?

Из средств обучения, используемых в системе открытого образования наиболее актуальным видится предоставление учебной информации в электронном виде, а также форум. Хорошим средством активизации процесса обучения является участие в учебных чатах. При этом заранее согласовывается его время со всеми участниками учебного процесса, обеспечивается достаточное быстродействие обмена информацией и выбирается наиболее спорная и актуальная тема для обсуждения в режиме реального времени. Наконец, весьма перспективным представляется использование видеоконференций, когда обучаемые лица видят друг друга и тьютора. При этом общение происходит уже не только на вербальном уровне, но и на уровне эмоций (удивление, загадочность, восторг и т.п.).

Таким образом, ясно, что применение дистанционных методов обучения – неизбежный этап развития системы образования. Процесс такого образования со временем совершенствуется. Электронные учебные пособия играют при этом важную роль. Однако диалог с тьютором позволит сделать ещё один важный шаг в совершенствовании процесса обучения. Кроме того, следует отметить, что применение электронных учебных пособий и система открытого образования не исключают, а дополняют друг друга.

В.А. Кадулин,
кафедра специальных информационных технологий
Московского университета МВД России

Совершенствование информационных систем оперативно-розыскного назначения

В условиях сложной криминальной обстановки, активизации деятельности организованных преступных формирований, зачастую приобретающей транснациональный характер, постоянного роста технического и финансового потенциала преступной среды совершенствование информационного обеспечения подразделений МВД России становится одним из главных направлений повышения эффективности правоохранительной деятельности.

В Программе МВД РФ «Создание единой информационно-телекоммуникационной системы органов внутренних дел»[1] указаны основные направления и механизмы повышения эффективности системы информационного обеспечения *органов внутренних дел* (ОВД).

Целью Программы стало создание *единой информационно-телекоммуникационной системы* (ЕИТКС) органов внутренних дел для повышения эффективности их деятельности на основе совершенствования системы информационного обеспечения ОВД посредством оборудования новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных телекоммуникационных, информационных и биометрических технологий. Это весьма актуально, поскольку около трети совершаемых в стране преступлений остаются нераскрытыми. Одной из причин такого положения является слабое информационное обеспечение оперативно-розыскной деятельности.

Между тем, роль розыскной информации в деятельности по раскрытию и расследованию преступлений, а значит и современных технологий её сбора, обработки и использования всё время возрастает. Потому необходимо создание единой информационно-телекоммуникационной системы ОВД, единой технологии обработки важной для органов расследования информации и разработка типовых программно-технологических решений по компьютеризации системы МВД России.

[1] Создание единой информационно-телекоммуникационной системы органов внутренних дел: Извлечение. Программа МВД РФ. Утверждена Приказом Министерства внутренних дел РФ от 08.07.2006 №420 // Организация правовой работы в системе МВД России. Сборник правовых актов и методических документов, том II, М., 2006.

Существующая система сбора и обработки значимой розыскной информации в виде локальных, региональных и федеральных картотек, коллекций и автоматизированных банков данных не в состоянии эффективно поддерживать деятельность по раскрытию, расследованию и профилактике преступлений. Это обусловливает необходимость совершенствования информационного обеспечения *оперативно-розыскной деятельности* (ОРД). Такой путь должен стать главным направлением решения многих служебных задач.

Целью настоящего исследования является определение направлений совершенствования информационного обеспечения оперативно-розыскной деятельности.

В интересах достижения данной цели в работе решаются следующие задачи:

1. Оценки значения розыскной информации в деятельности по раскрытию и расследованию преступлений.

2. Определения возможностей действующих *автоматизированных информационно-поисковых систем* (АИПС) и баз данных ОВД в решении задач информационного обеспечения оперативно-розыскной деятельности.

3. Разработки предложений по созданию информационных систем оперативно-розыскного назначения.

Успешное решение поставленных перед органами внутренних дел задач возможно лишь при широком применении средств компьютерной техники, а также при объединении всех коммуникаций в единую систему ОВД. При этом необходимо учитывать важность и особенности решения задач информационного обеспечения ОРД, приобретающих безусловную актуальность в связи с активизацией деятельности на территории России организованных преступных формирований и террористических группировок.

Выявление и изобличение таких преступников затрудняется из-за того, что имеющаяся в отношении них информация находится в ведении различных субъектов оперативно-розыскной деятельности. Сотрудники зачастую не осведомлены о том, что разрабатываемые ими лица представляют интерес для коллег из других служб и подразделений, а их разоблачение возможно, а в ряде случаев и необходимо, проводить совместными усилиями.

Затрачивая значительные силы и средства на добывание оперативно-справочной и криминалистической информации, органы внутренних дел не имеют чёткого механизма их централизованной автоматизированной регистрации, обработки и использования в раскрытии и расследовании преступлений.

Именно на данном направлении имеются незадействованные ресурсы, полное и качественное использование которых способно оказать значительное позитивное влияние на работу оперативных аппаратов и всей системы ОВД в целом. Учитывая, что имеющиеся в ОВД человеческие резервы повышения производительности труда уже практически исчерпаны, именно данному направлению работы должно в настоящее время уделяться самое пристальное внимание.

К сожалению, длительное отсутствие единой политики и централизованного контроля за состоянием информационного обеспечения оперативных служб привело к тому, что многие регионы начали эту работу значительно раньше, создали свои банки данных, реализованные на различных математических платформах, абсолютно не совместимые между собой по реквизитному составу, использующие различные технологии сбора, обработки и выдачи информации.

Организующей роли Главного информационно-аналитического центра (ГИАЦ) МВД России по данному направлению не просматривается, а государственное учреждение – научно-производственное объединение «Специальная техника и связь» (ГУ НПО «СТиС») за время своего существования никакого типового программного продукта для создания автоматизированных банков не создало. Наоборот, ведущиеся им в интересах различных служб НИОКР по данной линии работы были ориентированы на СУБД совершенно различного типа и таким образом ситуация только ухудшалась. Единственной программой, которая может претендовать на статус типовой, является автоматизированная информационно-поисковая система «АИС-УР», которая была создана по инициативе Департамента уголовного розыска и фактически закончена лишь в 2010 году.

Значительный объём информации, ежедневно проходящий через органы внутренних дел, вообще не закладывается ни в какие учёты. Это отказные материалы; лица, задерживаемые по подозрению в совершении преступлений; результаты осмотров мест происшествий; приметы разыскиваемых преступников и многое другое. Все эти сведения представляют интерес для оперативных работников, однако найти их при существующей системе учёта зачастую не представляется возможным.

Следует отметить, что даже существующие в настоящее время учёты остаются в должной мере не задействованными.

Особую актуальность приобрёл данный вопрос в связи с активизацией деятельности на территории России организованных преступных формирований и террористических группировок.

Во многих регионах не налажен доступ к базам данных других

правоохранительных структур, а также государственных органов и учреждений (регистрационной палате, пенсионному фонду, бюро технической инвентаризации и т.д.).

Выход из этой ситуации один – разработка и подписание соответствующих соглашений или совместных нормативных актов, однако в МВД России централизованно этой работой не занимается ни одно из подразделений, ответственных за организацию информационного обеспечения.

Низкая эффективность централизованных информационных фондов обусловлена сложностью непосредственного доступа конечного пользователя с его рабочего места к хранимой информации и, следовательно, недостаточной заинтересованностью практических работников в качественном заполнении большого количества часто изменяющихся (раз в 1-2 года) форм первичных документов. Это связано, прежде всего, с оторванностью сотрудников ОВД от процесса формирования банков данных и невозможностью получать самостоятельно в режиме реального времени имеющуюся в них информацию.

Преодолеть недостатки информационной работы в ОВД можно лишь на основе дальнейшего совершенствования её информационного обеспечения, базирующегося на современных информационных технологиях.

Информационное обеспечение в зависимости от области применения принято обозначать терминами «информационное обеспечение планирования», «информационное обеспечение деятельности руководителя», «информационное обеспечение инспекторских аппаратов» и др. Поэтому термин «информационное обеспечение» можно отнести как к функциям управления, так и к деятельности структурных подразделений или конкретных категорий сотрудников.

Информационное обеспечение должно позволять вводить, обрабатывать, хранить и получать необходимую информацию в зависимости от уровня управления, или от конкретного принимаемого управленческого решения. В свою очередь, информационное обеспечение любого конкретного направления деятельности ОВД заключается в тщательном отборе из всей совокупности информации только тех сведений, которые необходимы и достаточны конкретному сотруднику ОВД (субъекту управления) определённого уровня для эффективной организации его работы. Эти сведения должны быть предоставлены в нужный момент и в необходимом объёме, и непосредственно на его рабочее место.

Создание и функционирование названной системы на основе современных информационных технологий позволит решить задачу

обеспечения информационного взаимодействия с базами данных горрайорганов, системой информационного обеспечения МВД России и другими системами правоохранительных органов.

Правомерность и актуальность указанных задач системы информационного обеспечения подтверждается отечественным и зарубежным опытом создания систем информационного обеспечения и эксплуатации информационных систем. Этот опыт свидетельствует о том, что основным направлением развития системы информационного обеспечения должно быть расширение масштабов использования децентрализованной автоматизированной обработки информации, при этом объём децентрализованной обработки данных должен быть максимально возможным, а объём централизованной обработки только на необходимом уровне. Иными словами, речь идёт об оптимальном, целесообразном распределении функций системы информационного обеспечения горрайорганов.

С использованием информационных ресурсов «ИБД-Регион» за первое полугодие 2010 года раскрыто свыше пятьсот пятидесяти тысяч преступлений, что на шестьдесят семь процентов больше чем за аналогичный период 2009 года.

Помимо обеспечения оперативно-розыскной деятельности, на ГИАЦ МВД России в апреле 2010 года были возложены задачи по организации и координации деятельности подразделений МВД России в сфере формирования в Российской Федерации электронного правительства и переходу на предоставление (исполнение) государственных услуг (функций) в электронном виде. За короткий период времени с момента выполнения поставленных руководством Министерства задач, по данному направлению проделан значительный объём работ, а именно:

- обеспечена возможность заполнения электронной формы заявления о преступлении или правонарушении на Едином портале государственных услуг и передача его в органы внутренних дел; обеспечена возможность гражданина обращаться в органы внутренних дел с сообщениями о преступлениях или правонарушениях в электронном виде через сеть Интернет (с апреля по июнь 2010 года в МВД России поступило и направлено в МВД, ГУВД, УВД по субъектам Российской Федерации на рассмотрение и принятие мер 173 электронных сообщения);

- на едином портале государственных услуг обеспечена возможность подачи заявлений на проведение государственного технического осмотра транспортных средств через ссылки на Интернет-сайты территориальных подразделений ГИБДД в 73 субъектах Российской Федерации. В 2010 году через сеть Интернет по предварительной записи

поступило более 35 тысяч заявок на проведение технических осмотров. Более подробные и новые сведения о функциях и деятельности ГИАЦ МВД России, информация о предоставлении услуг населению имеются в сети Интернет на сайте МВД России.

Ещё одна проблема, которая требует особого внимания – это отсутствие системы передачи секретной информации по открытым каналам связи, которой могли бы пользоваться в повседневном режиме сотрудники оперативных подразделений всех уровней, причём как для передачи в МВД России секретных справок, так и информационных массивов, предназначенных для формирования федеральных банков данных.

Ещё в меньшей степени обеспечены каналами связи сотрудники территориальных ОВД. Практически во всех регионах возможностью пользоваться учётами в режиме реального времени обладают лишь подразделения, находящиеся в региональных центрах и около них. Большинство ГРОВД используют для этого телефонную связь, либо письменные запросы, срок выполнения которых занимает от 5 до 30 суток. Более того, эта линия работы не регламентируется никакими нормативными актами уровня МВД России и за неё практически никто не отвечает.

Часть региональных банков данных, представляющих повышенный интерес для раскрытия преступлений, не ведутся на федеральном уровне, что также оказывает негативное влияние на результативность борьбы с преступностью.

К их числу в основном относятся учёты, ведущиеся ГИБДД и миграционной службой, в том числе:

- зарегистрированные автотранспортные средства и их владельцы;
- специальная продукция, полученная от предприятий-изготовителей;
- похищенные и утраченные регистрационные, водительские документы и государственные регистрационные знаки;
- разыскиваемые транспортные средства, поставленные на оперативный учёт подразделениями ГИБДД (оперативный розыск);
- выданные заграничные паспорта и иные удостоверения личности;
- иностранные граждане и лица без гражданства, ищущие убежище на территории РФ (обратившие с ходатайством о признании беженцами на территории РФ или предоставлении политического убежища).

Наличие таких банков данных способно существенно повысить эффективность работы ОВД, так как факты использования преступниками поддельных документов и государственных номерных знаков для

автомобилей в настоящее время носят систематический характер.

Особую актуальность приобрёл данный вопрос в связи с активизацией деятельности на территории России организованных преступных формирований и террористических группировок.

Правовое регулирование информационного взаимодействия наряду с другими видами деятельности (сбор, обработка, хранение информации, доступ к базам данных информационно-поисковых систем и др.) в настоящее время выступает одной из важнейших проблем. Было бы не совсем справедливо утверждать, что в этом плане на сегодня мало, что сделано. Тем не менее, даже Федеральный закон «Об оперативно-розыскной деятельности» как универсальный многосубъектный акт, несовершенен. Именно нормы этого закона, в силу его специфики, должны закреплять, наряду с другими вопросами, исходные начала информационного взаимодействия. Тогда принимаемые в их соответствие подзаконные нормативные правовые акты вряд ли будут противоречить нормам данного закона.

Информационные системы, предназначенные для использования в органах внутренних дел, занимают особую нишу среди большого количества различных видов информационных систем регистрационного типа. Это связано в первую очередь с тем, что построение централизованных учётов в виде иерархической системы сбора, обработки, анализа и сопровождения информационных массивов основывается на документах первичного учёта, которыми как раз и оперируют информационные системы в ОВД.

Можно констатировать, что практически в любом подразделении ОВД сложилась парадоксальная ситуация – недостаток информации при её избыточности. Причина в том, что она не структурирована, не согласована, разрознена, не всегда достоверна, и её практически невозможно найти и получить в нужное время.

Почти все работы по созданию и развитию информационных систем направлены на формирование документальных информационных ресурсов и обеспечение доступа пользователей к ним. Тенденции развития современных информационных технологий приводят к постоянному возрастанию сложности автоматизированных информационных систем, создаваемых, как правило, на базе уже имеющихся приложений. Для успешной реализации новой информационной системы должны быть построены полные и непротиворечивые функциональные и информационные модели, что составляет логически сложную и трудоёмкую задачу. При этом необходимо учесть наличие традиционных приложений, связанных с обработкой транзакций и приложений аналитической обработки, использующих нерегламентированные запросы

к данным большого объёма.

В процессе создания информационных систем информационные потребности пользователей могут изменяться, что ещё более усложняет их разработку. Поэтому многие пользователи заинтересованы в комбинированном подходе, который бы позволил им воспользоваться достоинствами новых интегрированных баз данных, не отказываясь полностью от своих существующих и используемых учётов. Выходом из положения могут быть информационной системы, представляемые в виде конструктора баз данных, позволяющие легко создать новый вид учёта, при необходимости определить политику интеграции с уже существующими учётами.

Компромисс между противоречивыми требованиями может быть достигнут на основе применения интеллектуальных информационных систем, реализованных на основе баз знаний, способных объединить существующие базы данных центрального и регионального назначения ОВД. При этом определение набора базовых стандартов, которые комплексно объединяют интерфейсы, протоколы взаимодействия и форматы обмена данными, в принципе и составляет предмет функциональной стандартизации.

Литература

1. Конституция Российской Федерации // РГ от 25.12.1993 №237 (с посл. изм. от 21.07.2007 №5-ФКЗ // РГ от 27.07.2007).

2. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12.05.2009 № 537 // РГ от 19.05.2009 №88.

3. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // РГ от 29.07.2006 №165 (с изм. от 27.07.2010 №227-ФЗ // РГ от 02.08.2010 № 169).

4. Федеральный закон от 12.08.1995. № 144-ФЗ «Об оперативно-розыскной деятельности» // РГ от 18.08.1995 (с посл. изм. от 28.12.2010 №404-ФЗ // РГ от 30.12.2010 № 296).

5. Создание единой информационно-телекоммуникационной системы органов внутренних дел: Извлечение. Программа МВД РФ. Утверждена Приказом Министерства внутренних дел РФ от 08.07.2006 №420 // Организация правовой работы в системе МВД России. Сборник правовых актов и методических документов, том II, М., 2006.

6. Андреев Н.Д., Антонов В.В. Совершенствование системы информационного обеспечения сотрудников ОВД: Монография – Уфа: УЮИ МВД России, 2007.

7. Вершинин О.Е. Проблемные вопросы организации инфор-

мационного обеспечения оперативно-розыскной деятельности аппаратов УР. (Департамент УР МВД России), 2007.

8. Овчинский С.С. Оперативно-розыскная информация / Под ред. А.С. Овчинского и В.С. Овчинского. – М.: ИНФРА-М, 2000.

9. Оперативно-розыскная деятельность: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. – М.: ИНФРА-М, 2004.

10. Яковец Е.Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: Монография. – М.: Издательский дом Шумиловой И.И., 2005.

В.А. Кадулин,
кафедра специальных информационных технологий
Московского университета МВД России;
А.А. Кабанов, канд. юрид. наук, доцент

Компьютерная разведка в борьбе с преступлениями в сфере компьютерной информации

Впервые о проблемах борьбы с компьютерной преступностью в России отечественная криминалистическая наука официально заявила в июле 1992 года с момента проведения межведомственного семинара «Криминалистика и компьютерная преступность». Он был организован научно-исследовательским институтом Проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и Экспертно-криминалистическим центром МВД России. В течение последних 15-20 лет по мере компьютеризации хозяйственно-управленческой и финансово-коммерческой деятельности появились новые виды преступлений, которые стали называться компьютерными, исходя из терминологии зарубежной юридической практики.

Целью данной работы является определение направлений деятельности правоохранительных органов по раскрытию и предупреждению преступлений в сфере компьютерной информации методами и средствами компьютерной разведки.

Компьютерная разведка – сфера деятельности органов внутренних дел по гласному и негласному добыванию компьютерной информации[1]. Данное определение вытекает из задач подразделений ОВД. При широком и обобщённом взгляде на роль и место компьютерной

[1] Макаренков Д.Е. Лекция: Компьютерная разведка (введение в дисциплину). МосУ МВД России, М: 2008.

разведки в современном мире целесообразно воспользоваться следующим определением:

Компьютерная разведка – комплекс информационных технологий для систематического нахождения информации в открытых источниках и, возможно, доставки данных в машиночитаемой форме[1].

Подавляющее большинство юристов считает, что компьютерное преступление – это любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий. При этом к компьютерным преступлениям относится широкий круг действий, которые можно разделить на четыре категории: кража компьютерного оборудования; компьютерное пиратство (незаконная деятельность в сфере программного обеспечения); несанкционированный доступ к компьютерной системе в целях повреждения или разрушения информации; использование компьютера для совершения противозаконных или мошеннических действий.

Компьютерные технологии и международные компьютерные системы создали новые условия, которые содействуют совершению преступлений на национальном и международном уровнях.

Так, например, в США федеральный «компьютерный» закон действует уже с 1984 года, в Дании – с июля 1985 года, в Канаде – с декабря 1985 года, в Португалии – с 1982 года. Принятие соответствующих норм уголовного права осуществлено в Германии в августе 1986 года. Ведутся работы по усовершенствованию национального законодательства для борьбы с компьютерными преступлениями и в других странах мира[2].

В настоящее время существуют два основных направления научных исследований. Одно из направлений исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательств. В этом случае кража компьютера тоже является компьютерным преступлением. Другая часть исследователей утверждает, что объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства. Надо сказать, что законодательство многих стран, в том числе и в России, стало развиваться именно по второму пути.

---

[1] Кузнецов С.В. Разведка по открытым источникам для малого бизнеса // http://www.osint.ru/16osist.

[2] Виктор Сабадаш. Киберпреступность, кибертерроризм, кибервойна – как избежать электронного Ватерлоо // www. crime-research.ru, 22.09.2004.

В главе 28 Уголовного кодекса Российской Федерации определяются следующие общественно опасные деяния в отношении средств компьютерной техники:

1. Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

2. Создание программ для ЭВМ (или внесение изменений в существующие программы), заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ, или машинных носителей с такими программами.

3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ.

Следовательно, можно выделить следующие характерные особенности этого социального явления:

1) неоднородность объекта посягательства;

2) выступление машинной информации, как в качестве объекта, так и в качестве средства преступления;

3) многообразие предметов и средств преступного посягательства;

4) выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

На основе этих особенностей можно сделать вывод, что компьютерное преступление – это предусмотренное уголовным законом общественно опасное действие, совершённое с использованием средств электронно-вычислительной (компьютерной) техники.

Зарубежными специалистами разработаны различные классификации способов совершения компьютерных преступлений. Классификация и кодификатор компьютерных преступлений Генерального Секретариата Интерпола считается наиболее приемлемой в практике применения и признаны мировым сообществом. Названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола: несанкционированный доступ и перехват, изменение компьютерных данных, компьютерное мошенничество, незаконное копирование, компьютерный саботаж и прочие компьютерные преступления.

В настоящее время можно выделить основные группы мер предупреждения компьютерных преступлений: правовые и организационно-технические.

В группу правовых мер предупреждения компьютерных преступлений, прежде всего, относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере.

Организационно-технические меры предупреждения компьютерных преступлений целесообразно рассмотреть на примере мер, применяемых в развитых зарубежных странах.

Применение системы правовых и организационно-технических мер предупреждения компьютерных преступлений, несомненно, является одним из ведущих направлений в борьбе с компьютерными преступлениями. Однако хорошо известно, что одними мерами предупреждения (сдерживания) не всегда удается предотвратить преступное посягательство. Тем более что по единому мнению ведущих специалистов, занимающихся вопросами обеспечения безопасности компьютерных систем и электронного оборудования, в мире не существует абсолютно надёжных электронных систем, гарантирующих своим пользователям полную конфиденциальность и сохранность машинной информации, циркулирующей в них.

Относительная новизна возникших проблем, стремительное, наращивание процессов компьютеризации российского общества, по нашему мнению, застали врасплох правоохранительные органы, оказавшиеся неготовыми к адекватному противостоянию и активной борьбе с этим новым социальным явлением.

Как показывает практика, следователи, производящие расследование этой части компьютерных преступлений, сталкиваются со многими, подчас неразрешимыми трудностями, среди которых представляется необходимым выделить следующие:

- сложность квалификации преступных деяний;

- сложность в проведении различных следственных действий из-за несовершенства действующего уголовно-процессуального законодательства;

- сложность в назначении программно-технической экспертизы средств компьютерной техники и в формулировке вопросов, выносимых на рассмотрение эксперта;

- отсутствие по некоторым вопросам соответствующих специалистов, необходимых для привлечения в ходе следствия;

- отсутствие элементарных познаний в области компьютерных технологий и т.д.

Следует особо выделить факторы, оказывающие негативное влияние на процесс расследования компьютерных преступлений и требующие своего скорейшего решения:

1) несовершенство уголовно-процессуального законодательства;

2) крайне слабая нормативная база, призванная регламентировать правовой статус и специфические особенности информационных ресурсов;

3) отсутствие методик расследования преступлений указанного вида;

4) отсутствие обобщений следственной и судебной практики;

5) отсутствие базового экспертно-криминалистического центра по производству необходимых экспертиз *средств компьютерной техники* (СКТ);

6) отсутствие методик проведения криминалистических (программно-технических) экспертиз СКТ;

7) отсутствие учебно-методических центров для подготовки соответствующих специалистов для нужд правоохранительных органов;

8) крайне низкая оснащённость подразделений правоохранительных органов средствами компьютерной техники и региональная разобщённость при решении этих вопросов, вызванная нескоординированностью действий.

В результате совокупного взаимодействия указанных выше факторов на практике сложилась ситуация, которая существенно затрудняет возможность своевременного обнаружения преступления и полного сбора доказательств на первоначальном этапе работы по делу.

Как показывает анализ следственной практики, основной проблемой при выявлении и расследовании преступлений рассматриваемой категории является отсутствие у сотрудников минимально необходимых специальных познаний в этой области. Особенно много ошибок возникает при производстве следственных действий, которые, как правило, проводятся без участия соответствующего специалиста и без учёта специфики расследуемого преступления.

Неправомерный доступ к компьютерной информации представляет собой одно из самых малоизученных и в то же время довольно опасных преступлений последнего времени, приобретающее всё более угрожающие масштабы. Его последствия таят реальную опасность причинения вреда отношениям безопасности личности, общества и страны в самых разных сферах – от нарушения конституционных прав и свобод человека и гражданина до преступлений, посягающих на мир и международную безопасность.

Наметились серьёзные тенденции к использованию компьютер-

ной техники организованными преступными группами. Опасность схожих проявлений ещё более растет, когда участники организованных преступных групп получают доступ к *автоматизированным банкам данных* (АБД), обслуживающим системы государственной обороны, космонавтики, атомной энергетики и транспортного управления.

К новым явлениям, порождённым возможностью фактически безнаказанного совершения противоправных деяний, относятся хищения чужого имущества с внедрением электронно-вычислительной техники и средств электронного платежа. Они представляют серьёзную потенциальную опасность правам и законным интересам личности, общества и страны, хотя на современном этапе развития публичных отношений и не оказывают заметного влияния на состояние преступности в сфере экономики.

Неправомерный доступ к компьютерной информации – эпидемия транснационального характера. Об этом, в частности, свидетельствует тревожная тенденция к распространению последствий указанного деяния на межгосударственный уровень. Стремительно перешагнув границы отдельных стран, неправомерный доступ к компьютерной информации затрагивает интересы всего интернационального общества, причиняет вред и государствам, и народам, и конкретным людям.

Исходя из указанного, становится естественным, что неправомерный доступ к компьютерной информации как новая разновидность антиобщественного поведения представляет собой угрозу безопасности, нормальному функционированию общества и государства. Очевидно, что 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.

Более того, применение норм, содержащихся в ст. 272 УК РФ, будет неизбежно сопровождаться определёнными трудностями. Всё это может повлечь неоднозначное применение норм уголовного закона, устанавливающих юридическую ответственность за неправомерный доступ к компьютерной информации на практике и, следовательно, нарушить основополагающие принципы российского уголовного права – справедливости и законности. Понятно, что процесс юридической квалификации любого преступления состоит в установлении тождества наиболее существенных, обычных фактических событий конкретного общественно опасного и противоправного деяния признакам состава преступления определённого вида.

К настоящему моменту уже сформировались определённые схемы для хранения, обработки и утилизации знаний, связанных с объектами компьютерной разведки. Отработаны или будут вскоре отработаны методики эффективного применения этих знаний для решения конечных задач, вызванных потребностями оперативного анализа ситуации на рынке, сбора досье на его игроков, оценки эффективности PR-компаний и других сфер обеспечения безопасности бизнеса.

Подводя итог работы по определению направлений деятельности правоохранительных органов по раскрытию и предупреждению преступлений в сфере компьютерной информации методами и средствами компьютерной разведки, следует отметить, что проблема применения компьютерной разведки на различных этапах расследования и раскрытия преступлений в сфере компьютерной информации далека от разрешения. В работе удалось ответить на ряд вопросов, связанных с применением компьютерной разведки в борьбе с преступлениями в сфере компьютерной информации, а именно:

1. Определена степень общественной опасности компьютерной преступности и дана правовая оценка данному виду преступлений.

2. Рассмотрены технические и технологические характеристики преступлений в сфере компьютерной информации и указана основа противодействия данному виду преступлений.

3. Определена роль компьютерной разведки на различных этапах расследования и раскрытия преступлений в сфере компьютерной информации.

4. Выполнен анализ существующих средств компьютерной разведки, которые могут быть использованы в борьбе с преступлениями в сфере компьютерной информации органами внутренних дел.

В работе не удалось оценить существующие способы и средства мониторинга, тактические приёмы применения программных и аппаратных средств отслеживания и документирования действий правонарушителя в компьютерных системах.

Литература

1. Конституция Российской Федерации. Принята 12.12.1993 // РГ от 25.12.1993 №237 (с посл. изм. от 21.07.2007 №5-ФКЗ // РГ от 27.07.2007).

2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // РГ от 29.07.2006 №165 (с изм. от 27.07.2010 №227-ФЗ // РГ от 02.08.2010 № 169).

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // РГ от 17.06.1996 (с посл. изм. от 29.12.2010 № 442-ФЗ // РГ

от 31.12.2010 № 297).

4. Ермаков А.Е., Плешко В.В. Компьютерный анализ текста при сборе информации к досье из открытых источников. Доклад на 3-ей конференции «Конкурентная разведка в металлургии» (19-20 января 2005 г., Москва, гостиница «Балчуг Кемпински»). – М., 2005.

5. Сабадаш В. Киберпреступность, кибертерроризм, кибервойна – как избежать электронного Ватерлоо // www. crime-research.ru, 22.09.2004.

6. Макаренков Д.Е. Лекция: Компьютерная разведка (введение в дисциплину). – М.: МосУ МВД России, 2008.

Е.В. Клепикова,
начальник кабинета специальных дисциплин
кафедры специальных информационных технологий
Санкт-Петербургского университета МВД России

Информация, её полезность и восприятие

Человек придумал слова. Как в зеркале, в мозаике слов отразился окружающий мир: трава, цветы, шум прибоя, мерцание звезд, бесконечность галактик – и сам человек. Цепочки слов, замыкаясь в себе, образуют язык. Выражая в языке различные процессы, человек познает мир. Информация об окружающем мире необходима человеку так же, как воздух, вода, тепло. Представьте, что Вы оказались в замкнутом пространстве без света и звука, с абсолютно гладкими поверхностями. Вы почувствуете себя, по меньшей мере, неуютно. Отсутствие информации об окружающей действительности, времени, пространстве противоестественно для человека. Человек видит, слышит, осязает, чувствует запахи. Таким образом, можно сказать, что органы чувств человека служат для ввода информации, а именно:

- *зрение:* с помощью глаз люди различают цвета, воспринимают зрительную информацию, к которой относятся и текстовая, и числовая, и графическая;
- *слух:* уши помогают воспринимать звуковую информацию – речь, музыку, звуковые сигналы, шум;
- *обоняние:* с помощью носа люди получают информацию о запахах окружающего мира;
- *вкус:* вкусовые рецепторы языка дают возможность получить информацию о том, каков предмет на вкус – горький, кислый, сладкий, соленый;

• *осязание:* кончиками пальцев (или просто кожей), на ощупь можно получить: информацию о температуре предмета – горячий он или холодный, о качестве его поверхности – гладкий или шершавый.

Информация – это сообщение о состоянии и свойствах объекта, явления, процесса. Информация преобразуется уникальным устройством – человеческим мозгом и охватывает все сферы и отрасли общественной жизни, прочно входит в жизнь каждого человека, воздействует на его образ жизни, мышление и поведение. Она обслуживает общение людей, социальных групп, классов, наций и государств, помогает людям овладеть научным мировоззрением, разбираться в многообразных явлениях и процессах общественной жизни, повышать уровень своей культуры и образованности, усваивать и соблюдать законы и нравственные принципы.

Способы восприятия информации

По форме представления информацию делят на:

• *текстовую* информацию: например текст в учебнике, сочинение в тетради, реплика актера в спектакле, прогноз погоды, переданный по радио. Заметим, что в устном общении (личная беседа, разговор по телефону, радиопостановка спектакля) информация может быть представлена только в словесной, текстовой форме.

• *числовую* информацию: например таблица умножения, арифметический пример, счёт в хоккейном матче, время прибытия поезда и др. В чистом виде числовая информация встречается редко, разве что на контрольных по математике. Чаще всего используется комбинированная форма представления информации.

По общественному значению информация может быть:

• *личная* – это знания, опыт, интуиция, умения, эмоции, наследственность конкретного человека;

• *общественная* – общественно-политическая, научно-популярная, т.е. то, что мы получаем из средств массовой информации. Кроме того, это опыт всего человечества, исторические, культурные и национальные традиции и др.;

• *обыденная* – та, которой мы обмениваемся в процессе общения;

• *эстетическая* – изобразительное искусство, музыка, театр и др.;

• *специальная* – научная, производственная, техническая, управленческая.

Проблема поиска и использования информации – одна из самых актуальных в настоящее время, т.к. благодаря средствам массовых коммуникаций (печать, радио, телевидение, глобальные телекоммуникационные сети и т.д.) объём информации резко возрос. Это характер-

но абсолютно для всех сфер деятельности человека (наука, техника, политика, экономика и т.д.). Но в течение жизни человек может освоить лишь вполне определённое количество информации, что в сравнении с общим объёмом существующей информационной базы очень мало. Это обусловлено тем, что человеческий мозг не в состоянии хранить такой объём информации и без искажения передавать другим людям.

С развитием информационных ресурсов возникла необходимость представлять информацию в форме, отличающейся от привычной. Так, для передачи информации на расстоянии был изобретен телеграфный код Морзе, в котором буквы и цифры закодированы с помощью коротких и длинных импульсов (точка, тире). Почтовый индекс – закодированный адрес, считываемый автоматами, позволяет быстро и точно сортировать конверты. Вся вводимая в компьютер информация кодируется в двоичной системе счисления, таким образом любой символ (цифра, буква, знак) получает кодированное обозначение с помощью цифр 1 и 0, составляющих основу двоичной системы исчисления.

Писатели, поэты, музыканты, художники, учёные – каждый владеет своим профессиональным языком, недоступным для понимания непосвящённых, каждый по-своему объясняет мир. Однако это не мешает всем нам восторгаться результирующим продуктом их деятельности: стихотворением поэта, музыкой композитора, картиной художника, техникой, созданной учёными и изобретателями. Капитан корабля не может без риска провести корабль по фарватеру, не имея информации о последнем. Физик не сможет составить уравнение, не зная всех входящих в него величин. Приезжий без плана города с трудом ориентируется в незнакомой обстановке. Вся наша жизнь состоит из постоянного решения задач с неполной информацией. Чем больше информации, тем лучше можно управлять ситуацией. Во всех случаях информация выступает активным началом, позволяющим совершать необходимые действия. Иными словами, информация проявляется в процессе взаимодействия с неким устройством, которое будем называть управляющим. Без управления информация мертва, так же, как без информации не может правильно функционировать управление. Управляющим устройством может выступать человек, машина, программа, общество и т.д.

О.А. Кокорева, канд. юрид. наук. доцент,
доцент кафедры специальных информационных технологий
Санкт-Петербургского университета МВД России;
В.А. Кадулин,
кафедра специальных информационных технологий
Московского университета МВД России

Защита информации в процессе предупреждения недобросовестной конкуренции

Российское законодательство запрещает недобросовестную конкуренцию и рассматривает её как одну из форм деятельности, оказывающую негативное влияние на конкуренцию и направленную на ограничение конкуренции на товарных рынках.

Защита информации в процессе предупреждения недобросовестной конкуренции осуществляется на основе правового регулирования состава информации, относимой к коммерческой тайне.

В ряде случаев недобросовестная конкуренция осуществляется с целью захвата монопольного положения в какой-либо сфере предпринимательской деятельности или в каком-либо регионе. В настоящее время в Российской Федерации сформирована правовая база, позволяющая антимонопольным органам пресекать недобросовестную конкуренцию в административном порядке.

Федеральный закон РФ «О защите конкуренции» является основным законодательным актом, на основании которого антимонопольные органы осуществляют защиту от недобросовестной конкуренции[1].

Дело о недобросовестной конкуренции может быть возбуждено на основании заявлений коммерческих и некоммерческих организаций, федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления, представлений прокурора, а также по инициативе антимонопольных органов.

Федеральный закон «О защите конкуренции» определяет организационные и правовые основы защиты конкуренции, в том числе, предупреждения и пресечения:

1) монополистической деятельности и недобросовестной конкуренции;

[1] Федеральный закон РФ «О защите конкуренции» от 26.07.2006 № 135-ФЗ // РГ от 27.07.2006 № 162 (с посл. изм. от 29.11.2010 № 313-ФЗ // РГ от 03.12.2010 № 274).

2) недопущения, ограничения, устранения конкуренции федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, иными осуществляющими функции указанных органов органами или организациями, а также государственными внебюджетными фондами, Центральным банком Российской Федерации.

Целями этого Федерального закона являются обеспечение единства экономического пространства, свободного перемещения товаров, свободы экономической деятельности в Российской Федерации, защита конкуренции и создание условий для эффективного функционирования товарных рынков.

Федеральный закон «О защите конкуренции» распространяется на отношения, которые связаны с защитой конкуренции, в том числе с предупреждением и пресечением монополистической деятельности и *недобросовестной конкуренции,* и в которых участвуют российские юридические лица и иностранные юридические лица, федеральные органы исполнительной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления, иные осуществляющие функции указанных органов органы или организации, а также государственные внебюджетные фонды, Центральный банк Российской Федерации, физические лица, в том числе индивидуальные предприниматели.

Целью работы является анализ методов защиты информации в процессе предупреждения недобросовестной конкуренции на основе правового регулирования защиты информации, относимой к коммерческой тайне и другим видам тайн.

Недобросовестная конкуренция – это любые направленные на приобретение преимуществ в предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости и могут причинить или причинили убытки другим хозяйствующим субъектам – конкурентам либо нанести ущерб их деловой репутации.

Из определения недобросовестной конкуренции, содержащегося в ФЗ «О защите конкуренции», следует, что для признания действий недобросовестной конкуренцией они должны одновременно выполнять несколько условий, а именно:

- совершаться хозяйствующим субъектом;

- быть направлены на получение преимуществ в предпринимательской деятельности;

- противоречить положениям действующего законодательства,

обычаям делового оборота, требованиям добропорядочности, разумности и справедливости;

- причинить или быть способны причинить убытки другому хозяйствующему субъекту (конкуренту), либо нанести ущерб его деловой репутации (причинение вреда).

Согласно ст. 5 ГК РФ *обычаем делового оборота* признаётся сложившееся и широко применяемое в какой-либо области предпринимательской деятельности правило поведения, не предусмотренное законодательством, независимо от того, зафиксировано ли оно в каком-либо документе. При этом обычаи делового оборота применяются, если они не противоречат положениям действующего законодательства или договору.

В то же время термины «добропорядочность», «разумность», «справедливость» действующим законодательством не определены, в связи с чем эти термины следует применять в соответствии с их общим значением в русском языке. Термин «добропорядочный» толкуется как приличный, достойный одобрения, порядочный, а термин «порядочный», в свою очередь, как честный и соответствующий принятым правилам поведения[1].

Последним признаком недобросовестной конкуренции, указанным в её определении, является *причинение вреда* другому хозяйствующему субъекту-конкуренту. Такой вред может выражаться в убытках, которые терпит конкурент, и/или в ущербе его деловой репутации. При этом в обоих случаях для признания действий хозяйствующего субъекта недобросовестной конкуренцией достаточно одной лишь возможности наступления таких последствий и доказательств реального вреда не требуется.

Под *убытками* ст. 15 ГК РФ понимает расходы, которые лицо, чьё право нарушено, произвело или должно произвести для восстановления нарушенного права, утрата или повреждение имущества (реальный ущерб), а также неполученные доходы, которое это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода).

Практика показывает, что обычно недобросовестная конкуренция не приводит к утрате или повреждению имущества.

Вторым видом вреда, наступающего вследствие недобросовестной конкуренции, является *нанесение ущерба деловой репутации* конкурента. В условиях рынка деловая репутация предпринимателя явля-

[1] Толковый словарь русского языка под ред. СИ. Ожегова и Н.Ю. Шведовой – М., 1997.

ется одним из важнейших элементов коммерческого успеха, поскольку изменение репутации напрямую влияет на спрос, обращённый к хозяйствующему субъекту.

Под *деловой репутацией* обычно понимается сложившееся общественное мнение о профессиональных достоинствах и недостатках физического или юридического лица. Ущербом деловой репутации следует считать негативные изменения в такой оценке, что может выражаться, например, в изменении положительного мнения о лице на отрицательное, ухудшении мнения о деятельности лица, снижении к нему доверия со стороны контрагентов и покупателей.

Защита государственных и предпринимательских секретов в настоящее время является объективной необходимостью, которая определяется следующими причинами:

1) необходимостью обеспечения независимости и безопасности государства;

2) конкуренцией между объектами коммерческих предприятий;

3) преступными посягательствами на защищаемые законом экономические правоотношения в обществе.

Таким образом, объём охраняемых государством сведений расширился, в том числе – за счёт возрождения института коммерческой тайны[1]. Однако помимо коммерческой тайны за последний период появился ещё целый ряд различного рода сведений, подпадающих под юрисдикцию системы защиты информации.

В настоящее время в России подлежат защите не только государственные, но и другие секреты, прежде всего, коммерческая тайна.

Коммерческая тайна – это не являющиеся государственным секретом сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка информации) которых может нанести вред его интересам.

Современный Гражданский кодекс Российской Федерации в ст. 139 соотносит коммерческую тайну со служебной тайной и предусматривает гражданскую ответственность за их разглашение.

Некоторые из таких сведений также относятся к сфере различных видов тайн, только тайн иного рода по сравнению с государственными и коммерческими секретами. Необходимо сказать несколько слов и об этих категориях информации ограниченного распространения.

[1] Федеральный закон РФ «О коммерческой тайне» от 29.07.2004. № 98-ФЗ // РГ от 05.08.2004 №166 (в ред. Федерального закона от 02.02.2006 № 19-ФЗ, с посл. изм. от 24.07.2007 № 214-ФЗ // РГ от 01.08.2007).

На сегодня законодательством Российской Федерации установлены специальные режимы сбора, хранения и распространения следующих основных категорий информации, включающих различные виды сведений: а) государственные секреты (государственная тайна, служебная тайна, служебная информация); б) информация, отражающая различные аспекты общественной жизни (коммерческая тайна, конфиденциальные данные, журналистская тайна); в) информация в отношении частной жизни граждан (банковская тайна и тайна вкладов, врачебная тайна, тайна предварительного следствия, нотариальная тайна, тайна усыновления, тайна страхования, адвокатская тайна, сведения о мерах безопасности судей, должностных лиц правоохранительных и контролирующих органов)[1] и др.

Таким образом, налицо ещё несколько видов тайн, с объективным существованием которых государство обязано считаться и принимать надлежащие меры по их охране.

Противоборство конкурирующих государств за контроль над мировыми информационными ресурсами стало в настоящее время принципиально новой областью применения силового воздействия – так называемой «мягкой» силы. Если к настоящему времени мировое сообщество сформировало баланс сил, а также механизмы его поддержания и правового регулирования в области ядерных и обычных вооружений, то вопрос о паритете в области информационного соперничества остаётся открытым.

Единое информационное пространство мирового сообщества требует унификации информационных и телекоммуникационных технологий всех стран – субъектов информационного сообщества. Это даёт возможность мощным индустриальным державам усиливать своё политическое, экономическое и военное превосходство за счёт лидерства в информатизации и, в принципе, осуществлять глобальный информационный контроль над мировым сообществом, фактически навязывая свои социокультурные стандарты и правила жизнеустройства.

Несмотря на то, что в системе информационного обмена коммерческая тайна занимала одно из центральных мест, а ссылки на коммерческую тайну содержались более чем в сорока законах и подзаконных актах, долгое время она оставалась одним из самых неурегулированных институтов права в России. Упоминавшийся выше Указ Президента РФ № 188 по непонятным причинам выделял из состава коммерческой тайны «сведения о сущности изобретения, полезной модели

[1] См.: Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / Под ред. А.Ю. Шумилова. – М., 1997. С. 62-63.

или промышленного образца до официальной публикации информации о них» в отдельное понятие, что вызывало серьёзную путаницу, как у юристов, так и в фискальных органах.

Вторую попытку принятия Федерального закона «О коммерческой тайне» Госдума предприняла в 2003 г. 19 ноября закон был принят во втором и третьем чтениях. Вторая версия законопроекта предложила новое определение коммерческой тайны:

1) коммерческая тайна – конфиденциальность информации, позволяющая её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

2) информация, составляющая коммерческую тайну, – научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введён режим коммерческой тайны.

В отечественной правоприменительной практике неизвестно пока ни об одном прецеденте возмещения ущерба от утечки конфиденциальной информации и привлечения к уголовной ответственности за её разглашение. Это и не удивительно при столь длительном отсутствии должного правового регулирования[1].

Не всякое распространение не соответствующих действительности сведений, дискредитирующих другой хозяйствующий субъект, может быть признано актом недобросовестной конкуренции, а лишь такое, которое непосредственно способно оказать влияние на конкуренцию, то есть непосредственно предоставить лицу, распространившему информацию преимущества над конкурентами и причинить им вред.

Чаще всего данная форма *недобросовестной конкуренции* выражается в дискредитации конкурента. Обычно дискредитация имеет своей целью подрыв доверия клиентуры (потребителей или иных контрагентов) к конкуренту или его продукции и привлечение потребителей к собственной продукции путём распространения ненадлежащей информации, в число которой входит и неполная информация о

[1] См.: *Гостев И.М.* Защита коммерческой тайны: история и современность // Электронное периодическое издание ЭЛ № 77-8528. 2004.

конкуренте, его товарах и услугах. Результатом данного проявления недобросовестной конкуренции является уход потребителей от «опороченного» конкурента к другим хозяйствующим субъектам, при этом не обязательно в полном объёме к лицу, распространившему порочащую информацию. Следовательно, в данном случае преимущества выражаются в притоке новых потребителей.

Можно выделить три признака рассматриваемой формы недобросовестной конкуренции:

- распространение информации;
- её недостоверность;
- причинение вреда.

Вред может выражаться в убытках или ущербе деловой репутации.

Ущерб деловой репутации может наступить, во-первых, в результате распространения порочащих лицо сведений. Во-вторых, на репутацию хозяйствующего субъекта могут оказать влияние сведения, хотя и не порочащие его репутацию, но содержащие негативную оценку его деятельности, например, об уровне подготовки кадров. Объектом дискредитации также могут стать товары или услуги. В такой ситуации, распространяемая информация обычно содержит утверждения о низком качестве товара, несоответствии их установленным требованиям, отсутствии специальных разрешений, если такие требуются.

Помимо дискредитации к данной форме недобросовестной конкуренции относится также распространение информации, которая хотя и не наносит ущерба деловой репутации другого хозяйствующего субъекта, но способна причинить ему убытки.

Учитывая изложенное, антимонопольные органы используют обязанность коммерческих и некоммерческих организаций предоставлять информацию антимонопольным органам и запрашивать у лица, распространившего информацию, документы, подтверждающие соответствие действительности сведений, способных нанести вред другому лицу.

Получение, использование, разглашение информации, составляющей коммерческую, служебную тайну и иную охраняемую законом тайну, отличается от рассмотренных форм недобросовестной конкуренции, связанных с информацией, в данном случае объектом действий является достоверная информация. Закон упоминает три вида такой информации:

- коммерческая;
- служебная;
- иная охраняемая законом тайна.

То есть, речь идёт об информации, доступ к которой ограничи-

вается на основании действующего законодательства.

Коммерческая тайна может содержаться, в частности, в научных произведениях (отчётах, заключениях и др.), заявках на выдачу патента на изобретение, полезную модель, в конструкторской, технологической, товаросопроводительной документации, договорах, контрактах, списках поставщиков, заказчиков, клиентов.

К коммерческой тайне может быть отнесена информация, включающая методы производства и его организации, химические формулы, рецептуры, опытные образцы, а также методы сбыта и распространения продукции, контракты, планы деятельности, рекламная стратегия, сведения о потребителях, списки поставщиков или заказчиков (клиентов).

Информации, составляющей служебную и коммерческую тайну, посвящена ст. 139 ГК РФ, согласно которой для отнесения информации к служебной или коммерческой тайне необходимо, чтобы она имела коммерческую ценность в силу её неизвестности третьим лицам, к ней не было свободного доступа на законном основании, а обладатель принимал меры к охране её конфиденциальности. Под коммерческой ценностью информации следует понимать случаи, когда её использование может увеличить доходы лица, в том числе, путём снижения издержек на производство.

Закон не указывает на субъекта, чьи действия по *разглашению информации* третьим лицам могут считаться недобросовестной конкуренцией. Однако из определения недобросовестной конкуренции следует, что это хозяйствующий субъект:

1. Во-первых, им может быть контрагент владельца информации, у которого информация оказалась на законном основании, но право передачи информации третьим лицам у него отсутствует.

2. Во-вторых, распространить чужую конфиденциальную информацию может конкурент, получивший информацию также без согласия владельца. В данной ситуации действия конкурента напрямую направлены на сведение к минимуму коммерческой ценности информации конкурента и причинение ему тем самым ущерба. Ослабление позиций конкурента, соответственно, производится в расчёте на привлечение к себе новых клиентов.

Рассмотренные действия могут быть признаны недобросовестной конкуренцией только в том случае, если они совершаются без разрешения владельца информации.

Следует также отметить, что закон не указывает лицо, чья конфиденциальная информация должна неправомерно использоваться, следовательно, им может быть не только конкурент, но и другой хо-

зяйствующий субъект.

Проявления недобросовестной конкуренции в рекламе выражается при продвижении товаров на рыке в целях увеличения сбыта и развития конкуренции. Поэтому одной из основных целей Закона «О рекламе»[1] является защита от недобросовестной конкуренции. Перечень форм недобросовестной конкуренции, приведённый в Законе «О конкуренции» тесно перекликается с перечнем форм ненадлежащей рекламы.

С другой стороны, сообщение верных по существу сведений также может при определённых обстоятельствах вводить в заблуждение.

Таким образом, анализируемая норма вводящей в заблуждение рекламы запрещает сообщение не объективно неправильных (неверных) сведений, а субъективно неправильных, т.е. способных ввести в заблуждение. Это означает, что для установления введения в заблуждение в смысле Федерального закона «О рекламе» единственным критерием должно быть только субъективное восприятие рекламы.

В рекламе недопустимо и *злоупотребление доверием физических лиц*. Следует отметить, что на сегодня в России существует целый ряд лиц или организаций, которым в силу определённых обстоятельств доверяют широкие круги населения. От них потребители ждут независимых оценок и объективных мнений. И если должностные лица, ссылаясь на объективность своего мнения, используют этот статус с целью побудить потребителей приобрести определённые товары или услуги, они тем самым злоупотребляют доверием населения и действуют неправомерно. Не случайно Федеральный закон «О рекламе» содержит запрет на распространение в рекламе не соответствующих действительности сведений в отношении прав на использование государственных символов, а также символов международных организаций.

В некоторых странах использование преувеличения квалифицируется как введение в заблуждение. Российский законодатель прямо не называет рекламные преувеличения вводящими в заблуждение сообщениями.

Законодательство разных стран не всегда рассматривает преувеличения в рекламе как одну из форм недобросовестной конкуренции.

Российское рекламное законодательство исходит из принципа, что потребители воспринимают серьёзно все рекламные утверждения, особенно те, в которых товар представляется как уникальный («самый», «абсолютно», «единственный» т.д.) и, следовательно, предусма-

[1] Федеральный закон РФ от 13.03.2006 № 38-ФЗ «О рекламе» // РГ от 15.03.2006 (с посл. изм. от 28.09.2010 № 243-ФЗ // РГ от 30.09.2010 №220).

тривает очень строгие критерии.

Реклама, *порочащая имя и репутацию предпринимателя,* признается Законом «О рекламе» недобросовестной. Такая реклама, в которой используются некорректные сравнения в отношении конкурентов (их товаров) или содержатся высказывания (образы), задевающие честь, достоинство и деловую репутацию конкурентов, не допускается.

Таким образом, Закон содержит ограничения по распространению так называемой сравнительной рекламы, а также утверждений, дискредитирующих конкурента.

Если сравнения в рекламе способны вызвать неверные представления у потребителей по поводу предлагаемого товара, она будет рассматриваться как ненадлежащая. Федеральный закон «О рекламе» запрещает некорректные сравнения рекламируемого товара с товаром (товарами) других юридических или физических лиц.

В соответствии с Законом «О рекламе» недостоверной является реклама, в которой присутствуют не соответствующие действительности сведения в отношении: товаров, самого рекламодателя, его правомочий и обязательств.

Очевидно, что понятие недостоверной рекламы ограничивается ложными утверждениями, которые могут создать неверное представление у потребителей относительно рекламируемого товара или услуги. Это, в свою очередь, может привести к серьезным последствиям и нанести вред как здоровью, так и имуществу граждан или юридических лиц.

Закон возложил функции контроля за соблюдением ограничений на рекламу на государство, как гаранта прав граждан, а именно на Федеральную антимонопольную службу России, а также её территориальные подразделения.

Федеральный закон «О защите конкуренции» регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау). Кроме того, этот закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной её конфиденциальности с целью обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну.

Положения этого Федерального закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида

носителя, на котором она зафиксирована.

Следует отметить, что его положения не распространяются на сведения, отнесённые в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Таким образом, существующая законодательная база России в существенной мере обеспечивает защиту информации в процессе предупреждения недобросовестной конкуренции. Но, при этом, правоприменительная практика противодействия недобросовестной конкуренции в нашей стране пока недостаточно развита и эффективна.

Литература

1. Большой энциклопедический словарь. 2-е изд., пер. и доп. – М.: Большая Российская энциклопедия, 2000.

2. Федеральный закон РФ «О коммерческой тайне» от 29.07.2004 № 98-ФЗ // РГ от 05.08.2004 №166 (в ред. Федерального закона от 02.02.2006 № 19-ФЗ, с посл. изм. от 24.07.2007 № 214-ФЗ // РГ от 01.08.2007).

3. Федеральный закон РФ «О защите конкуренции» 26.06.2006 № 135-ФЗ // РГ от 27.07.2006 №162 (с посл. изм. от 29.11.2010 № 313-ФЗ // РГ от 03.12.2010 №274).

4. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // РГ от 29.07.2006 №165 (с изм. от 27.07.2010 №227-ФЗ // РГ от 02.08.2010 № 169).

5. Федеральный закон РФ от 13.03.2006 № 38-ФЗ «О рекламе» // РГ от 15.03.2006 (с посл. изм. от 28.09.2010 № 243-ФЗ // РГ от 30.09.2010 №220).

С.В. Кондратенко,
преподаватель кафедры специальной техники ОВД
Санкт-Петербургского университета МВД России

GRID-технологии и возможность их использования при осуществлении сложных математических вычислений для решения задач, стоящих перед органами внутренних дел

Понятие, исторические истоки и суть GRID-технологий

Термин GRID (переводится как решетка или как вычислительная сеть) только недавно начал входить в лексикон специалистов по информационным технологиям. Однако аналитики уже сейчас прогно-

зируют, что идея GRID может радикально изменить мир информационных технологий, точно также как когда-то это сделал Интернет.

Понятие GRID было разработано Яном Фостером, Карлом Кессельманом и Стивом Тьюком. Они также стояли и у истоков формирования первого стандарта конструирования GRID-систем, свободно распространяемого программного инструмента с открытым кодом Globus Toolkit. Этот стандарт объединил в себе не только управление хранением данных, но и управление процессорным временем, движениями данных, обеспечением безопасности, контролем состояний, а также инструменты для разработки дополнительных сервисов. Впервые полнофункциональные прототипы GRID-систем стали использоваться в проекте Distributed Computing System (DCS) project вначале 70-х годов, над которым велись работы в Калифорнийском Университете под руководством Дэвида Фарбера. Суть технологии выглядела следующим образом: *сеть*, работающая как одна очень гибкая система, на которой отдельные узлы (компьютеры) могут запрашивать задачи. Однако в 1980-х годах данная технология была практически полностью заброшена, так как сложности администрирования и вопросы безопасности, связанные с выполнением задачи на компьютере, который не контролируется человеком, казались (и до сих пор могут казаться) непреодолимыми.

Сегодняшняя реальность любой организации такова, что под любое новое коммерческое приложение покупается новый компьютер (компьютеры), что приводит к появлению множества слабо связанных между собой вычислительных «островков». Связывание их в единый «континент» даже в рамках одной организации позволило бы резко повысить эффективность использования оборудования и уменьшить количество компьютеров в организации. Имея такой суперкомпьютер неограниченной мощности, любой пользователь может в любое время и в любом месте попросить столько вычислительных ресурсов, сколько ему требуется (и сколько он может оплатить), решить свои задачи и освободить ресурс.

Часто в связи с концепцией GRID также используют термин «виртуализация». Действительно, GRID представляет собой не множество мелких компьютеров, а один виртуальный суперкомпьютер, не с множеством дисков, на которых лежат файлы и базы данных, а с единой виртуальной областью хранения данных (огромным «виртуальным диском»), который образуется из множества отдельных дисков. Итак, с точки зрения пользователя GRID, не важно, где размещаются данные, и какой компьютер будет обрабатывать его запросы, главное – это то,

что пользователь потребовал информацию или выполнение вычислений и получил результат.

Вычислительная GRID – это программно-аппаратная инфраструктура, которая обеспечивает из любого места в мире надежный, согласованный и недорогой доступ к высокоэффективным вычислительным ресурсам. «Недорогой», поскольку имеется возможность использования в качестве элементов GRID недорогие вычислительные элементы с недорогой операционной системой, что, в свою очередь дает толчок развитию коммерческого использования GRID вычислений.

Если со стороны пользователя GRID все просто (попросил ресурс – получил его), то со стороны организаций, предоставляющих этот единый вычислительный ресурс, необходимо обеспечить выполнение ряда требований.

Необходимо обеспечить выделение вычислительных ресурсов, которые, в свою очередь полностью используются, т.е. не должно возникать ситуации, когда пользователь будет ждать выделения ресурса. Ещё более сложная задача – сделать информацию, необходимую для выполнения вычислений, доступной в то время, когда она необходима, и в том месте, где она необходима. Так, если речь идет о быстрой переброске огромных баз данных в ту часть света, где есть свободные вычислительные мощности, то сегодня эта задача не выполнима, так как скорость и пропускная способность сетей передачи данных в большинстве своём ограничены техническими параметрами. Но в рамках предприятия и ограниченного числа файлов и баз данных решить эту задачу можно.

Необходимо также обеспечить постоянную доступность и работоспособность системы GRID. Выход из строя отдельных её элементов не должен останавливать работу приложений.

Возможности применения GRID-технологий в системе ОВД.

На основании вышеизложенного, представляется целесообразным и эффективным решением применить GRID-технологии, не только используя глобальные ресурсы Интернета для решения научных задач и проведения исследований, но и в локальных вычислительных сетях отдельных ведомств (если такие сети содержат достаточное количество отдельных рабочих станций – например, несколько тысяч).

Так, на примере ГУВД по городу Санкт-Петербургу и Ленинградской области, имеющему в своём распоряжении большое количество компьютеров, объединённых высокоскоростной шиной передачи данных на основе оптоволокна, в перспективе целесообразно организовать работу GRID-технологий для использования значительных вычислительных мощностей и применять их для практического расчёта

сложных математических моделей, таких как:

- организация дорожного движения и работы светофоров в городе, учитывая динамично меняющуюся обстановку, в зависимости от времени суток, дня недели, проведения общегородских и специальных мероприятий;

- планирование координации работы специальных служб и всех отделов и подразделений ГУВД при возникновении чрезвычайных ситуаций, в том числе массовых беспорядков;

- планирование организации работы систем видеонаблюдения на городских улицах, режимных предприятиях и охраняемых объектах, с целью её систематизации и получения оперативного доступа к необходимым фрагментам по территории города и временнЫм промежуткам;

- планирование, расстановку, расчёт сил и средств в процессе обеспечения безопасности (в том числе от угрозы террористических актов), а также при обеспечении массовых мероприятий, требующих привлечения значительного количества сотрудников ОВД, обеспечения их оружием, боеприпасами и специальной техникой.

В настоящее время на практике вышеуказанные модели, с использованием ЭВМ не рассчитываются, так как требуют дорогостоящего машинного времени суперкомпьютеров, а, следовательно, значительных материальных затрат. Использование GRID-технологий позволит создать такие компьютерные мощности на основе уже существующей материальной базы, с неизмеримо меньшими затратами и высокой эффективностью полученных результатов.

В.В. Кутузов, канд. техн. наук, доцент,
доцент кафедры *специальных информационных технологий*
Санкт-Петербургского университета МВД России;
В.А. Кадулин,
кафедра специальных информационных технологий
Московского университета МВД России

Проблемы противодействия организованной преступности в информационной сфере

В настоящее время борьба с преступлениями в сфере информационных технологий является третьим по счёту приоритетом в деятельности ФБР США после борьбы с терроризмом и контрразведкой.[1]

[1] http://www.fbi.gov/priorities/priorities.htm

В Российской Федерации до недавнего времени считалось, что компьютерная преступность – явление, свойственное только зарубежным странам, и по причине слабой компьютеризации нашего общества, отсутствует вообще. Именно это обстоятельство и привело к отсутствию сколько-нибудь серьёзных научных исследований этой проблемы.

Цель работы: формулирование проблем противодействия организованной преступности в информационной сфере и определение путей их разрешения.

Для достижения поставленной цели в работе решаются следующие задачи:

1. Анализа и оценки существующих методов и средств противодействия организованной преступности в информационной сфере.

2. Определение направлений противодействия организованной преступности в информационной сфере (в области правовой, организационной и технической).

3. Разработка предложений по противодействию организованной преступности в информационной сфере.

Организованная преступность – наиболее опасная форма преступности, выражающаяся в создании и деятельности организованных преступных групп и преступных организаций. Организованная преступная группа – объединение двух и более лиц в устойчивую управляемую группу для совершения преступлений.

Участник преступной организации – лицо, умышленно принимающее участие в деятельности преступной организации или оказывающее содействие в разработке или реализации мер по осуществлению такой деятельности либо созданию условий для её поддержания и развития.

Быстрое развитие новых информационно-коммуникационных технологий по всему миру имеет и свою негативную сторону: создаются возможности для появления новых форм эксплуатации, новых разновидностей преступной деятельности и даже новых форм преступности. Для того, чтобы адекватно реагировать на возникающие угрозы, предпринимаются усилия по борьбе с компьютерными преступлениями, как на национальном, так и на межгосударственном уровнях.

Развитие новых информационных технологий в современном мире является не только фактором прогресса, но и имеет свою негативную сторону: создаются возможности для появления новых форм эксплуатации, новых разновидностей преступной деятельности и даже новых форм преступности.

Об этом свидетельствует ряд международных документов, из

которых выделяются следующие: Конвенция о киберпреступности, принятая 27 апреля 2000 года Советом Европы; Меры по борьбе против преступлений, связанных с использованием компьютеров, принятые на Одиннадцатом Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями в Бангкоке 25 апреля 2005 года; Окинавская Хартия глобального информационного общества, принятая 23 июля 2000 года на Окинаве (Япония) на совещании руководителей Глав государств и правительств стран «Группы Восьми».

В силу того, что наибольшей юридической силой среди указанных документов обладают нормы универсальных документов более подробно остановимся на документах Одиннадцатого Конгресса ООН: *противодействие компьютерной преступности.*

Существует ряд связанных с использованием компьютеров преступлений, объектом которых являются собственно информационно-коммуникационные технологии. Иногда такого рода преступления классифицируются как преступления против конфиденциальности, целостности или доступности компьютерных систем. К таким преступлениям относятся различные виды незаконного использования услуг электросвязи и незаконного использования компьютерных услуг путём применения разного рода хакерских технологий.

Мировые эпидемии компьютерных вирусов в последние двадцать лет нарушали работу сетей, обслуживающих компании и потребителей, а время от времени ситуация ещё более осложнялась вследствие появления новых, особенно мощных и вредоносных штаммов «червей» и вирусов.

Важно также знать, каким образом компьютеры используются как инструменты или орудия для совершения преступлений. Существует множество видов преступлений, связанных с изменением данных; некоторые из них (как, например, электронный вандализм) предполагают преступно причинённый вред (порча веб-сайта), а другие представляют собой профессионально выполненные подлоги или подделки.

Хищение данных может быть не только экономическим преступлением: недавно появившаяся категория преступлений, связанная с хищением личных данных, может также нарушать право на неприкосновенность частной жизни и смежные права физических лиц.

Существует много видов преступлений, связанных с использованием компьютеров, в рамках которых имеет место хищение денежных средств: это, например, атаки хакеров на банки или финансовые системы либо мошенничества, связанные с переводом «электронных денег». Высказывалась также озабоченность по поводу электронного отмыва-

ния денег и сопутствующих ему проблем, таких как уклонение от уплаты налогов.

Такие «традиционные» виды преступлений, как вымогательство (угроза разгласить частную информацию или личные данные либо нанести ущерб данным или системам) и преследование, также существуют и в «сетевых» вариантах.

В последние годы всё больше внимания уделялось связи между терроризмом и Интернетом, хотя и здесь имеют место разноплановые процессы. Существуют признаки того, что Интернет используется для содействия финансированию терроризма, а также в качестве инструмента планирования и осуществления террористических актов. Всё больше внимания уделяется и роли Интернета в пропаганде терроризма, а также его использованию для вербовки.

Существуют два чётких основания для беспокойства: посягательства на важнейшие данные и посягательства на важнейшие элементы инфраструктуры. Всё глубже осознается зна́чимость важнейших элементов информационной инфраструктуры, сетей, которые не только дают возможность поддерживать связь, но и используются для управления и контроля над важнейшими составляющими других ключевых элементов инфраструктуры, таких как энергетика, транспорт, продовольственное снабжение и здравоохранение. Во многих странах мира важнейшие элементы инфраструктуры могут находиться в частной собственности и быть особенно уязвимыми, поскольку многие их распределённые системы контроля и системы диспетчерского контроля и получения данных *подключены* к Интернету, через который их функционирование можно нарушить.

Важно иметь возможность противостоять атакам (по мотивам терроризма или других видов преступной деятельности), направленным на важнейшие элементы информационной инфраструктуры, с тем, чтобы свести к минимуму серьёзный риск цепной реакции, которая затрагивает другие наиболее необходимые элементы инфраструктуры, имеющие важное значение для общества.

Глобальная компьютеризация современного общества породила новую сферу общественных отношений, которая, к сожалению, нередко становится объектом противоправных действий со стороны организованных преступных групп.

Компьютерные преступления всё более приобретают организованный и групповой характер, а иногда, и транснациональный. Транснациональный характер компьютерной преступности на сегодня составляет определённую общественную опасность, реально угрожая информационной безопасности – составляющей национальной безопас-

ности государства. Современные технологии дали толчок не только свободной торговле и экономической деятельности, но и стимулировали преступную деятельность.

Как уже было отмечено выше, при расширении сферы использования информационных технологий и различных технологических процессов, возрастает и количество правонарушений с использованием компьютерной техники.

Объективно это объясняется снижением уровня защищённости информационных систем, увеличением количества антисоциальных проявлений вследствие увеличения количества пользователей глобальных компьютерных систем, использовании научных и технических достижений криминалитетом. Интересы организованных преступных групп направлены на отмывание денег, добытых преступных путём, распространение заведомо ложной информации, финансовые махинации, и в первую очередь, в кредитно-банковской сфере, где активно используются автоматизированные системы [2].

Преступления, совершаемые организованными преступными группами с использованием информационных технологий, можно разделить на две большие группы:

1) преступления ненасильственного, как правило, экономического характера;

2) преступления насильственного характера.

К преступлениям ненасильственного, экономического, характера, совершаемым организованными преступными группами путём использования информационных технологий, можно отнести:

- отмывание денег, добытых преступным путём;
- мошенничество с платёжными пластиковыми карточками;
- хищение денег с банковских счетов;
- кибератаки с целью хищения информации;
- фальшивомонетничество;
- компьютерное мошенничество;
- распространение детской порнографии;
- распространение наркотиков.

Организованная экономическая преступность – это глобальная социальная проблема практически всех экономически развитых государств и крупных международных субъектов. По оценкам международного валютного фонда масса «грязных денег» составляет от 590 до 1500 млрд. долларов, то есть от 2 до 5 % суммарного ВВП всех стран мира [3]. Закономерная цель организованной группы – получение криминальных капиталов и их легализация, т.е. введение их в сферу легальной предпринимательской деятельности. «Отмывая грязные день-

ги», организованные преступные группы всё чаще используют всемирную компьютерную сеть Интернет.

Отмывание денег с помощью Интернет подразумевает использование всемирной паутины для того, чтобы скрыть происхождение денег, полученных нелегальным путём. Отмывание денег – давно известное преступление, однако анонимность Интернета облегчила преступникам осуществление махинаций с «грязными деньгами», помещение их в легальные активы и инвестиции.

Можно назвать следующие способы отмывания денег через Интернет: проведение азартных игр; использование Интернет-банков. С помощью проведения азартных игр, в Интернете незаконно полученные доходы используются для заключения сделок в играх на деньги. Интернет–банки также предоставляют возможности для преступников, которые могут открыть счёт, не общаясь «лицом к лицу» с работниками банка. Деньги могут быть депонированы на секретный оффшорный счёт в банке или перемещены с помощью электронных переводов из одного банка в другой, и так далее, пока след найти станет трудно или практически невозможно. Хотя всё ещё остается трудность с помещением большой суммы наличных денег на счёт, но если уж эта сумма помещена, то перемещать её и управлять ею намного быстрее и легче чем раньше – посредством электронного перемещения.

Всё большего распространения получает такой вид преступления, как мошенничество с платёжными пластиковыми карточками, возникшее в 1990-е годы. Этот вид преступлений отличается простотой, отсутствием насилия, а также тем, что потерпевшие – банк и законный собственник карты, как правило, никогда не видят преступника. Данный вид мошенничества также широко используется организованной преступностью. По данным Генерального секретариата Интерпола, почти 60% всех мошенничеств, связанных с использованием кредитных карточек, совершены организованными преступными группами азиатского происхождения, а на преступные группы из Нигерии. Болгарии, Ирана и стран бывшего Советского Союза приходится 40% совершений этого вида преступлений [4].

Существенную область противодействия организованной преступности в информационно-психологической сфере занимают проблемы выявления, расследования и предотвращения компьютерных преступлений. Если преступные информационно-психологические воздействия и даже информационные атаки в социальной, экономической и политической сферах ещё не нашли отражения в законотворческой деятельности, то любое компьютерное преступление представляет собой факт нарушения той или иной нормы уголовного или гражданского

права [6].

Показателен опыт создания структуры по противодействию нарушениям в сфере авторского права на музыкальные произведения – Международной Федерации Производителей Фонограмм (IFPI) [6].

IFPI – организация, представляющая интересы звукозаписывающей индустрии. Членами IFPI являются около 1400 производителей и распространителей музыки в 76 странах, IFPI также осуществляет деятельность с присоединившимися промышленными ассоциациями в 48 странах (Европа – 23, Азия, – 10, Америка – 9, Африка – 4, Австралия и Новая Зеландия).

Задачи IFPI:

- борьба с музыкальным пиратством;

- содействие открытому доступу на музыкальный рынок и обеспечение правовой защиты авторских прав;

- содействие и развитие благоприятных условий и новых технологий для звукозаписывающей индустрии в период становления цифровых технологий;

- пропаганда роли музыки в развитии экономики, в социальной и культурной жизни.

Членом IFPI может стать любое юридическое или физическое лицо, производящие музыкальные записи и музыкальное видео в достаточных количествах. IFPI осуществляет меры по противодействию пиратству и защите авторских прав в индустрии звукозаписи. В 2001 году было завершено формирование региональных офисов и офисов в отдельных странах. Посредством их IFPI сотрудничает с органами полиции и таможни. Данное взаимодействие рассматривается IFPI как одно из ключевых в решении задач организации.

При непосредственном содействии IFPI в раде стран были проведены мероприятия по пресечению нарушений авторского прав и смежных прав. Наиболее масштабные в 2001 году мероприятия проведены в Нидерландах, Мексике и Польше.

В 2002 году в Интерполе, совместно с представителями IFPI и общественности, сформирована рабочая группа по преступлениям против интеллектуальной собственности.

В то же время правовая квалификация компьютерных преступлений может вызвать существенные затруднения, и чёткую границу между информационными атаками и компьютерными преступлениями провести чрезвычайно сложно.

Особенности компьютерных преступлений обусловлены высоким быстродействием электронных систем и пространственным размахом телекоммуникационных сетей. Компьютерные преступления мож-

но совершать за доли секунды, находясь на любом удалении от собственно места преступления, т.е. объект посягательства может быть атакован преступником, находящимся на другой стороне земного шара. Последнее подтверждает тот факт, что эффективное противодействие организованной преступности в информационной сфере возможно только в рамках международного сотрудничества.

Специальными исследованиями, с моделированием компьютерных атак на тестовые объекты и изучения последующей реакции атакуемых предприятий и учреждений, проведёнными в США в 1990-е годы, установлено, что факты взлома были зафиксированы лишь в 2-5 % случаев. Т.е. фиксируемые компьютерные преступления, совершённые с использованием технологий удаленного доступа – это лишь малая часть успешных, а тем более проводимых попыток несанкционированного доступа к компьютерным системам.

В Российской Федерации в 2003 году по сравнению с предыдущим отмечен рост с 4232 до 7782 (т.е. в 1,8 раза) количества выявленных преступлений по признакам главы 28-й Уголовного кодекса «Преступления в сфере компьютерной информации» [5]. Факторами успешного выявления правоохранительными органами Российской Федерации данного количества нарушений можно также считать учёт особенностей совершения преступных действий против компьютерной информации непосредственно в диспозициях уголовных статей 28-й главы Уголовного кодекса (термины «копирование», «модификация»), а также создание и использование системы СОРМ.

Успешное решение проблемы противодействия организованной преступности в информационной сфере и борьбы с ней возможно при условии учёта международного опыта и на основе создания национальной системы противодействия преступлениям, связанным с использованием компьютеров в Российской Федерации.

Литература

1.Азаров Л.С. Проблемы усовершенствования ответственности за «компьютерные» преступления: концептуальный подход // Уголовное право: стратегия развития в XX1 веке. М.: Проспект, 2005. С. 304-307.

2.Астахов А., Сухаренко А. Кибертерроризм: мифы и реалии // Новые криминальные реалии и реагирование на них. – М.: Российская криминологическая ассоциация. 2005. С. 186-193.

3.Батурин Ю.М., Жодзинский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 2006.

4.Быстряков Е.Н., Иванов А.Н., Климов В.А. Расследование компьютерных преступлений. – Саратов. 2007.

5.Овчинский А.С. Нетрадиционные подходы противодействия организованной преступности на основе информационных технологий // Информационно-аналитический журнал «Факт», 2000, №7.

6.Яблоков Н.П. Криминалистическая характеристика финансовых преступлений // «Вестник Московского университета», Серия 11, Право, 2004. №6.

7.Яковец Е.Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: Монография. – М.: Издательский дом Шумиловой И.И., 2005.

8.Яковлев А.Н. Возможности компьютерно-технической экспертизы // Вопросы квалификации и расследования преступлений в сфере экономики. Саратов, 2004.

А.Ю. Лабинский, канд. техн. наук, доцент,
СПбУ ГПС МЧС России

Информационные технологии как основа дистанционного образования

Использование ЭВМ в учебном процессе позволяет повысить качество обучения за счёт высокой дидактической эффективности, обеспечения опережающей подготовки специалистов для перспективных направлений, использования активных форм самоподготовки слушателей и применения ЭВМ для контроля текущей успеваемости.

К середине 2000 года большинство организаций и специалистов пришли к единому мнению о необходимости создания и развития в России системы *дистанционного образования* (ДО), под которой понимается комплекс образовательных услуг, предоставляемых населению с помощью передовых информационных, компьютерных и иных технологий в рамках специализированной информационно-образовательной среды, базирующейся на средствах обмена информацией. В системе Госкомвуза была разработана «Концепция создания и развития дистанционного образования в России».

Большинство представителей вузов России отмечает перспективность и эффективность средств ДО как одной из форм высшего образования, обеспечивающей выход в международную систему образования и расширения профессиональных контактов, а также более полного использования научно-методического потенциала российской высшей школы и привлечение дополнительных средств для финансирования учебной и научной деятельности вузов.

Наиболее значимым элементом ДО в своём вузе представители

вузов России считают заочное обучение на базе ДО, так как виртуальная образовательная среда обеспечивает возможность как индивидуальной ориентации на каждого обучаемого, так и групповой (поточной) ориентации.

Наибольшие затруднения в использовании ДО, по оценкам экспертов, вузы испытывают в научно-методическом обеспечении, в создании электронных учебных курсов, банков информации по учебным дисциплинам, а также в подготовке преподавателей для работы с сетевыми технологиями в качестве консультантов (тьюторов).

К настоящему времени накоплен немалый опыт в построении отдельных программных компонентов, автоматизирующих работу бухгалтерии, учебного отдела и т.п. Однако учебных материалов в электронном виде сравнительно немного, а доступ к ним требует определённой квалификации.

Таким образом, создание и накопление электронных источников информации наравне с упрощением процедуры доступа к ним является актуальной задачей. Особое место занимают вопросы администрирования процесса ДО и регламентации доступа, то есть определение системы правовых отношений.

Анализ возможных путей построения системы ДО на компьютерных сетях позволил выделить ряд базовых направлений её реализации:

- ориентация системы ДО на российские регионы;
- использование транспортной среды TCP/IP;
- создание и развитие сети региональных учебных центров;
- создание подсистемы сетевого администрирования ДО;
- подготовка преподавательского состава для работы в сетевой среде;
- методологическая переработка учебных курсов для системы ДО.

Таким образом, каждый учебный курс представляет собой совокупность учебных материалов, которые должны быть изучены обучаемым. В процессе обучения проводится многократное тестирование с передачей результатов тестирования в административный центр системы ДО.

Представленный подход предполагает, что виртуальная образовательная среда обеспечивает возможность как индивидуальной ориентации на каждого обучаемого, так и групповой (поточной). При групповой организации обучения обучаемые объединяются в виртуальную группу независимо от места их проживания. Все члены виртуальной учебной группы получают доступ в групповую телеконференцию, где они могут проводить коллективные дискуссии и обмениваться мнениями, не встречаясь лично. Такие конференции позволяют зна-

комить обучаемых с информацией, предназначенной для данной группы, а также отвечать преподавателю на типовые вопросы обучаемых. Кроме того, любой обучаемый имеет возможность обратиться по электронной почте к преподавателю и получить компетентный индивидуальный ответ.

Индивидуальная ориентация системы ДО на обучаемого обеспечивается следующими функциями системы ДО:

- создание специального файла с описанием полномочий данного слушателя;
- индивидуальный контроль за ходом освоения материала каждым обучаемым;
- сбор статистики о результатах прохождения тестов по каждому курсу;
- возможность переноса информации об успеваемости в другие подсистемы;
- организация двусторонней связи слушателей и преподавателей через электронную почту.

При переработке учебного курса в электронный источник информации к последнему должны быть предъявлены следующие требования:

- активизация познавательной деятельности обучаемых;
- управление познавательной деятельностью обучаемых;
- полнота представления учебной информации;
- адаптация электронного источника информации к уровню подготовки слушателей;
- дружественный диалоговый режим работы;
- семантическая и техническая надёжность электронного источника информации;
- открытость электронного источника информации;
- простота описания и работы с электронным источником информации;
- обеспечение безопасности информации и защиты от несанкционированного доступа.

В 2005 году исследовательская группа социологов лаборатории социальных проблем современного общества социологического факультета Московского государственного университета провела опрос 35 экспертов-представителей различных вузов России. Целью исследования было изучение востребованности форм и методов системы ДО в вузах. Проведённое исследование показало, что:

- в ведущих вузах имеются условия для активизации усилий по внедрению элементов ДО;

- ДО может быть использовано как самостоятельная форма заочного обучения;

- большинство вузов не готово в полной мере к полноценному развертыванию и функционированию элементов ДО;

- необходима федеральная программа развития системы ДО в стране, а также разработка комплексных программ развёртывания ДО в высшей школе;

- необходимо совершенствовать организацию и методы социологического мониторинга как средства управления оптимизацией развития системы ДО в высшей школе.

Появившаяся в 2003 году архитектура Microsoft.NET – это новая технология разработки программного обеспечения. В её основе лежит идея обеспечения универсальности программного кода, что даёт возможность работы программы на любой платформе (при условии, что платформа поддерживает технологию .NET).

В эпоху стремительного развития глобальной информационной сети Интернет, объединяющей компьютеры различных архитектур, важнейшими задачами при создании программного обеспечения становятся:

- переносимость (возможность выполнения на различных типах компьютеров);

- безопасность (невозможность несанкционированных действий);

- надёжность (способность сохранять работоспособность в различных условиях);

- межъязыковое взаимодействие (возможность использовать несколько языков программирования).

Архитектура Microsoft.NET позволяет успешно решать все эти задачи, и основана на множестве разнообразных спецификаций и инициатив. Использование архитектуры Microsoft.NET для создания методического обеспечения ДО позволяет решить вопросы: переносимости, безопасности, надёжности работы такого программного обеспечения.

Таким образом, создание ДО в высшей школе предоставляет большие возможности для дальнейшего развития традиционно устоявшихся форм образования на новый качественный уровень.

Литература

1. Программа «Организация и развитие системы очного и заочно-дистанционного образования», утвержденная приказом Министерства общего и профессионального образования РФ №260 от 29 октября 1998 г.

2. Артамонов В.С., Лабинский А.Ю., Примакин А.И. Дистанционное обучение как новый этап развития заочного образования:

Учеб. пособие. – СПб ун-т МВД РФ, 2000.

3. Богданов М.И., Гадышев В.А., Лабинский А.Ю. Автоматизированное учебное рабочее место. Учебно-методич. пособие. – СПб Высшая пожарно-техническая школа МВД РФ, 1995.

4. Лабинский А.Ю., Кабанов А.А. Возможности компьютерной графики как средства информатизации учебно-воспитательного процесса // Правовая информатика: Материалы выступлений на заседании 20 секции 28 международной конференции «Школьная информатика и проблемы устойчивого развития» в Санкт-Петербургском университете МВД России. Санкт-Петербург, 25 апреля 2009 г. / Сост. и ред. А.А. Кабанов. – СПб.: СПб ун-т МВД России, 2009. – С. 68-73.

5. Лабинский А.Ю. Программное обеспечение проведения автоматизированного контроля текущей успеваемости // Правовая информатика: Материалы выступлений на заседании 20 секции 28 международной конференции «Школьная информатика и проблемы устойчивого развития» в Санкт-Петербургском университе¬те МВД России. Санкт-Петербург, 25 апреля 2009 г. / Сост. и ред. А.А. Кабанов. – СПб.: СПб ун-т МВД России, 2009. – С. 74-75.

6. Лабинский А.Ю. Использование новых информационных технологий для решения вопросов методического обеспечения учебного процесса // Новые информационные технологии и информационная безопасность: Межвузовский сб. научных статей. Вып. 1 / Под ред. А.А. Кабанова. – СПб.: СПб ун-т МВД России, 2010. – С. 30-32.

7. Ногин С.Б. Автоматизированные учебные курсы и их разработка. – СПб.: ВАС, 1999.

И.Г. Мишуткин, курсант 723 учебного взвода;
Н.А. Виноградова, старший преподаватель
кафедры специальных информационных технологий
Санкт-Петербургского университета МВД России

ICQ – новый вид межличностных коммутаций

Мы живем в мире, где самой большой ценностью является информация. Однако информация быстро устаревает. Её быстрое обновление требует соответствующей системы связи. Для этого была создана компьютерная сеть.

Сначала она делала робкие шаги и объединяла отдельные компьютеры в пределах комнаты или здания. Далее появились сети, объединявшие компьютеры в разных частях городов и даже стран. Следующим шагом стало объединение этих сетей между собой. Так

появился Интернет – сеть, объединяющая локальные сети.

Но для такой структуры, как Интернет, требовались несколько иные способы связи и коммуникации. Время требовало нового вида связи, более совершенного. Этот способ должен был быстро помочь найти в сети нужного человека. Поэтому продукт никому не известной в тот момент израильской фирмы Mirabilis, появившийся на свет в 1996 г., почти сразу перевернул все имеющиеся представления о способах связи и общения в Интернете.

ICQ – это запись английской фразы «I seek you» «I seek you», которая переводится, как «я ищу тебя».

ICQ стала первой программой из целой плеяды Интернет-пейджеров, завоевавшей бешеную популярность во всем мире. Сервер Mirabilis, через который осуществлялись распространение клиента и связь, буквально трещал под напором желающих немедленно скачать эту программу.

Принцип работы этой программы прост. Пока Вы не подключаетесь к Интернету, ICQ тихо «дремлет» в дальнем уголке памяти компьютера. Но как только Вы входите в сеть, она пробуждается и посылает на сервер сигнал — «Объект номер такой-то вошел в сеть». Сервер в тот же момент пересылает этот сигнал Вашим знакомым (если, конечно, у них имеется собственный экземпляр ICQ, и они заблаговременно внесли ваш номер в так называемый «контакт-лист»).

В результате спустя несколько секунд после вашего входа в Интернет Ваши знакомые узнают об этом.

Основная функция ICQ – мгновенный обмен сообщениями, но есть так же и множество других, не менее интересных возможностей, предлагаемых этим сервисом.

Работая с ICQ, можно отправить через её собственный сервер электронное письмо (и даже ярко раскрашенную поздравительную открытку) любому человеку из вашего «контакт-листа», причём получено оно будет сразу же после входа Вашего абонента в Сеть. Через ICQ можно передать вашему собеседнику файл или голосовое сообщение.

Если захотелось найти себе новых друзей по интересам, то Вы можете зарегистрироваться на сервере ICQ и внести свое имя и координаты в один из многочисленных списков. В дополнение ко всему ICQ снабдит Вас собственной домашней страничкой – на ней Ваши знакомые смогут найти только самые краткие сведения о Вас и номер вашей ICQ.

Программа ICQ вовсе не была построена сразу «от и до», подобно многим коммерческим программным продуктам. Когда разработчикам ICQ приходила в голову новая идея по усовершенствованию

программы, они просто добавляли новый модуль в уже существующую версию. Когда большое количество пользователей ICQ высказывало пожелания относительно реализации какой-нибудь новой функции, разработчики брались за дело и выполняли эти пожелания.

Новшества, которые добавляют в ICQ авторы, весьма и весьма полезны – например, последние её версии умеют автоматически напоминать о днях рождения ваших знакомых, позволяя при этом отправить и красивую «виртуальную открытку», снабжены собственной системой поиска информации в сети…

Нельзя забывать о том, что, помимо основных функций ICQ, можно легко получить ещё с десяток другой дополнительных. Новые возможности для ICQ воплощены в виде дополнительных программ-модулей (plug-ins), которые можно скачать на сайте разработчика. Так, система ICQ Surf поможет вам общаться с пользователями ICQ, оказавшимися на каком либо сайте одновременно с вами. Другой плагин позволит сохранять ваш контакт-лист в Интернете, на специальном сервере, с которого его можно в любой момент восстановить…

Сама программа (помимо своей основной функции – обмена мгновенными сообщениями) поддерживает ещё и целый ряд удобных сервисов, не уступающих основному по качеству и оперативности. Например, выделив мышкой файл (или группу файлов) на своём компьютере, пользователь может тут же отправить их своему собеседнику (или группе собеседников). В том случае, если пользователю нужно отправить e-mail, он просто щёлкает мышкой по адресату, и почтовая программа стартует, автоматически написав адрес e-mail (указанный в данных адресата) собеседника в поле «Кому».

Работая в ICQ, можно воспользоваться также услугами ICQ-почты. Эта бесплатная почтовая служба работает аналогично почте Hotmail или Yahoo! Для того чтобы отправить или принять электронную почту, не обязательно соединяться с сервером ICQ. Даже в этом случае можно пользоваться адресной книгой или отправлять вложенные файлы.

При наличии на компьютере полнодуплексной звуковой карты и после установки на компьютер соответствующего программного обеспечения посредством ICQ возможно голосовое общение с другими пользователями этого сервиса (желательно, чтобы скорость связи с Интернетом была не ниже 19200).

Сервис ICQ включает в себя так называемые сообщества для объединения людей со схожими интересами. Вообще, ICQ – это отличный способ найти новые знакомства в сети. Ко всему вышеперечисленному следует добавить поддержку сетевых игр, возможность

оперативного поиска нужных людей в сети и бесплатность этой программы. Вот почему сервис ICQ пользуется просто феноменальным успехом и почему уникальный идентификационный номер (UIN) пользователя (который выдается при регистрации) стало принято указывать на визитных карточках.

Программа ICQ – это очень хороший способ общения, как на больших расстояниях, так и на малых. Ясно, что программа ICQ уже прижилась в нашем обществе и многие люди не могут без неё обходиться. Установив и запустив на своём компьютере программу ICQ, пользователь приобретает свой интернет-коммуникатор и может открыть для себя Интернет в совершенно ином свете.

А.В. Пономаренко, канд. пед. наук, доцент,
доцент кафедры специальных информационных технологий
Санкт-Петербургского университета МВД России

Задачи государства по обеспечению реализации информационных прав физических лиц в сети Интернет

К настоящему времени основные направления развития законодательства в информационной сфере определены, в основном соответствуют зарубежной практике правового регулирования информационных отношений и осуществляются в соответствии с международно-правовыми требованиями к обеспечению свободы слова и иных прав и законных интересов граждан в области производства, хранения и распространения информации.

В России интенсивное использование информационных технологий опережает реакцию законодателя, которому требуется время для адекватной регламентации в законах и иных нормативных правовых актах отношений, возникающих в рассматриваемой сфере. Кроме того, очень важно разумно учитывать опыт других стран, которые, значительно раньше приступив к освоению информационного пространства, и в частности к борьбе с преступлениями в сфере высоких технологий, выработали систему эффективных правовых средств этой борьбы.

На современном этапе законодательные инициативы должны затрагивать два основных направления регулирования в информационной деятельности общества:

информационное экономическое право (регулирует порядок осуществления в информационной сети электронной экономической деятельности: электронной торговли, Интернет-банкинга, электронного консалтинга, электронной рекламы, Интернет-страхования и т.д.);

информационное гуманитарное право (регулирует порядок осуществления в информационной сети электронной гуманитарной деятельности по обеспечению государством реализации информационных прав физических лиц, в том числе путём создания и функционирования систем электронного администрирования).

Одним из направлений здесь является развитие существующих более чем в 30 странах мира так называемых систем электронного правительства (управления). Несмотря на принятие соответствующих концепций и развития системы электронного правительства, существует много проблем, и в основном правового характера. К 2017 году поэтапно предполагается выдать всем дееспособным гражданам России пластиковую карту, с помощью которой можно будет совершить большинство уведомительных, регистрационных и платёжных операций через «инфоматы». В рамках этой системы реализация прав граждан на оказание им публичных услуг осуществляется органами государства с помощью глобальных компьютерных сетей. В частности, уже сейчас граждане получают возможность через специальные сайты государственных органов в сети Интернет получать доступ к соответствующей публичной информации о деятельности этих государственных органов, обращаться с жалобами и обращениями, направлять заявки на выдачу всевозможных справок, разрешений, оказание услуг социального характера.

Но недостаточное информирование общества вызывает неадекватные действия со стороны граждан, недостаточно осведомлённых в сфере информационных технологий, и в сфере своих прав на защиту персональных данных.

Указанная система должна способствовать упрощению диалога между обществом и властью, повышать эффективность и адресность государственного и муниципального управления. Другим направлением выступает обеспечение государством информационных прав граждан, в том числе на свободный оборот незапрещённой (находящейся в открытом доступе) информации, её сбор, обработку и распространение в электронной форме.

Необходимо также создание и совершенствование сетевого законодательства, регулирующего: сетевые безналичные расчёты для подготовки перехода к электронным деньгам, сетевое взаимодействие для дистанционного заключения договоров, сетевое разрешение споров в виртуальных процессах и многое другое.

Особо необходимо отметить, что приоритетным направлением развития законодательства Российской Федерации должна стать проблема охраны прав человека в условиях формирования информацион-

ного общества.

Особое внимание необходимо уделять недостаточно разработанным в законодательстве РФ вопросам:

реализации права на информацию;

формированию эффективной системы информирования общества и совершенствованию функционирования средств массовой информации;

совершенствованию законодательства в области предпринимательства, прежде всего в части новых видов деятельности, таких, как электронная торговля, работа, обучение;

дальнейшей либерализации рынков информационных продуктов, технологий и услуг, развитию конкуренции;

защите персональной тайны;

охране интеллектуальной собственности;

улучшению сетевого доступа к информационным ресурсам и защите информации в сетях передачи данных.

И естественно, информация, превращаясь в основные ресурсы развития общества, должна защищаться государством. С этой целью законодательство обязано стоять на страже интересов граждан, обеспечивать правовую защиту на всех уровнях взаимодействия в новых условиях жизнедеятельности информационного общества.

И.В. Степанов, канд. юрид. наук, доцент,
доцент кафедры специальной техники ОВД
Санкт-Петербургского университета МВД России

Современное состояние и характерные особенности компьютерной преступности

Современный период развития нашего государства характеризуется не только относительно высоким количественным ростом преступности в целом, но и её качественным изменением. Развитие высоких технологий позволяет большей части населения иметь персональные компьютеры, сотовые телефоны, модемы и иные средства связи, что не только свидетельствует об уровне мобильности общества, но и создаёт условия для появления новых форм и видов злоупотреблений техническими средствами, в том числе и в преступных целях.

В настоящее время компьютерная преступность характеризуется постоянным увеличением качественных и количественных показателей, высоким уровнем латентности данных общественно опасных деяний, возможностью причинения значительного ущерба и сущест-

венного вреда.

Непрерывный рост числа компьютерных преступлений вызван объективными условиями технического прогресса, одним которых является практическая невозможность человека всесторонне предвидеть появление новых компьютерных вирусов и способов совершения данного вида преступных деяний, а значит своевременно и квалифицированно выработать противодействие в отношении них.

Изучение данных уголовно-правовой статистики свидетельствует о ежегодном увеличении таких видов преступлений во всем мире. В развитых странах с высоким экономическим развитием и компьютеризацией компьютерная преступность имеет долгую историю, и борьба с ней давно признана одной из первостепенных задач государства, поскольку при совершении указанных правонарушений экономике страны наносится огромный ущерб.

Среди основных причин быстрого роста и актуализации данного вида преступлений в первую очередь следует отметить их высокий уровень латентности, а также сверхвысокий уровень обогащения в течение короткого времени. Также этому способствуют и объективные трудности, связанные не только с выявлением и документированием рассматриваемых правонарушений, но и с их доказыванием, что делает преступления в сфере компьютерной информации привлекательней год от года для всё большего числа лиц.

Особенностью компьютерных преступников является сравнительно молодой возраст, а также высокий уровень знаний новых компьютерных технологий, которые молодым поколением усваиваются значительно легче. Наличие специального образования для компьютерного преступника не является обязательным атрибутом. Тем не менее, абсолютное большинство преступников имеют среднее и высшее образование. При этом более чем у 50% лиц, совершивших преступление в сфере компьютерной информации, имеется специальная подготовка в области автоматизированной обработки информации.

С появлением глобальных компьютерных сетей, например, сети открытого доступа Интернет, компьютерные преступления могут совершаться в одном государстве, а преступный результат наступить в другом, причём следы преступлений могут оказаться в ряде третьих государств. В этих случаях необходимы разработка и принятие целого ряда международных нормативно-правовых актов, которые должны регулировать отношения в компьютерной сфере на межгосударственном уровне и способствовать разрешению споров и конфликтов в данной области.

Одной из причин, способствующих развитию компьютерной

преступности, является поведение жертвы преступления, а именно принятие решения потерпевшей стороны об обращении в правоохранительные органы по факту совершения компьютерного преступления, которое зачастую делается неохотно в связи с различными обстоятельствами. Кроме этого, зачастую, средства массовой информации создают у граждан, и в первую очередь у молодёжи, неправильное представление об ответственности за совершение компьютерных преступлений, об институте интеллектуальной собственности, создают неадекватный образ компьютерного преступника.

Воздействие на преступность, деятельность по её предупреждению необходимо расценивать как систему, включающую различные элементы, например:

1) объекты профилактики – социальные явления и процессы разных уровней, обусловливающих состояние и структуру преступности (причины и условия), а также определённые категории лиц (правонарушители и потерпевшие);

2) субъекты профилактики – совокупность государственных и общественных органов, учреждений и социальных институтов;

3) мероприятия и профилактические меры, осуществляемые субъектами профилактики в отношении её объектов.

В свою очередь, государству следует сформировать политику безопасности, направленную на обеспечение:

- конфиденциальности информации;
- целостности информации;
- готовности к использованию информации и средств её обработки.

Не в последнюю очередь должны совершенствоваться и меры непосредственно технического предупреждения компьютерной преступности, к которым можно отнести такие, как разработку новейших систем защиты информации от несанкционированного доступа и физическую защиту крупнейших компьютерных центров от нападений террористов.

Ввиду активного развития сети Интернет с целью более эффективной борьбы с компьютерной преступностью, необходимо использование и обобщение опыта правоохранительных органов разных стран, а также сотрудничество и выработка совместных мероприятий по предупреждению данного вида преступности. С учётом многочисленности объектов компьютерной преступности и с целью повышения эффективности противодействия и раскрытия преступлений в сфере компьютерной информации, целесообразно создание в системе правоохранительных органов особых групп специалистов по борьбе с компьютерными преступлениями. В настоящее время данные функции

выполняют сотрудники управления «Р».

Подводя итог вышесказанному в целях повышения защиты от компьютерных преступлений необходимо:

- своевременное получение информации о совершении преступлений в исследуемой сфере и используемых при этом новых методов, с целью их изучения и своевременного реагирования;
- создать центр помощи потерпевшим от компьютерных преступлений, способствующий восстановлению испорченных или утраченных программ, представляющих материальную ценность;
- разработать государственную программу по финансированию систем, противодействующих несанкционированному доступу в информационные системы;
- всесторонне и достоверно освещать в средствах массовой информации компьютерные преступления и последствия их совершения.

И.И. Ушаков, канд. техн. наук, доцент,
Дом Ученых им. М. Горького РАН

К нелинейным взаимодействиям поляризационно-магнитооптических эффектов в дисперсных системах

В стабильных атомах нарушения симметрий пространства-времени исследовались в нашей стране И.Б. Хрипловичем «Несохранение чётности в атомных явлениях» М., Наука, 1981 [1], и за границей М.-А. Бушье, Л. Потье «Оптические эксперименты и слабые взаимодействия» [2]. Этот обзор опубликован в журнале «Успехи физических наук», где на странице 301 сформулировано обоснование, что «… взаимодействия слабых нейтральных токов нарушают чётность, и поэтому следует ожидать нарушений чётности также и в стабильных атомах». В указанной монографии И.Б. Хрипловича на стр.4 аннотации, также подтверждены возможности физических исследований слабых взаимодействий оптическими методами.

Специально разработанная экспериментальная техника унополярных импульсных магнитных полей позволила впервые операционально непосредственно измерить без оптического компенсатора пространственную физическую величину (магнитоэллиптичность), всегда сопутствующую эффекту Фарадея (время).

Последующие также операциональные исследования с использованием дополнительного магнитоэллиптического модулятора (линейная четвертьволновая кристаллическая кварцевая пластинка в металлическом экране между импульсным соленоидом модулятора и ос-

новным) позволили непосредственно измерять в такой сдвоенной фарадеевской ячейке указанные физические величины при минимальных значениях напряжённости магнитных полей и даже при изменении их знака (направления), то есть при перевороте спинов микрочастиц определённых иерархических уровней. Угловые величины пространства-времени в таких условиях переполюсовки одного из магнитных полей принимают максимальные значения, что вероятно, соответствует наибольшим перепадам энергии даже с обострением при учёте самодействия внутринуклонных микрочастиц.

Нелинейные с обострением увеличения некоторых измеряемых величин углов пространства-времени при изменении полярности одного из магнитных полей на нашей модели теоретически можно объяснить самодействием скалярных полей Хиггса [3]. В нашем случае экспериментально измеряются уже не спонтанные нарушения симметрий пространства-времени, а чётко детерминированные магнитными полями нарушения угловых симметрий пространства-времени при указанных переполюсовках магнитных полей. Для подтверждения необходимо было исследовать особенности взаимодействия с органическим стеклом (ПММА) лазерного излучения различных видов поляризации (линейно поляризованного, эллиптической и магнитоэллиптической поляризации) при воздействии на этот образец импульсов магнитного поля различной напряжённости и положительной ориентации (рис. 1).

Так, при одинаковом механическом повороте поляризатора 3 или плоскости поляризации оптически активным веществом вправо или влево от нулевого положения до ОК 6 (см. рис. 2) на+\-225 угловых минут на исследуемый образец, уже после ОК 6 вместо линейно поляризованного излучения поступает эллиптически поляризованное излучение различной величины и знака (различной симметрии) в соответствии с известными измерениями, но ориентация азимута большой оси эллипса поляризации на выходе ОК 6 остается практически в неизменном положении (проверено экспериментально). Для линейно поляризованного излучения и обычной эллиптической поляризации противоположных знаков величиной (225+1) угловых минут эффект Фарадея в указанном образце из оргстекла при линейном увеличении напряжённости магнитного поля изменяется линейно (график 1, рис.1).

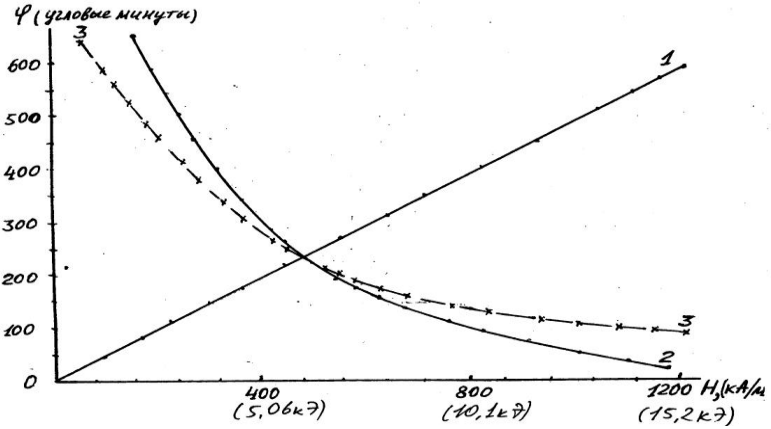

Рис. 1. Измерение (в органическом стекле) эффекта Фарадея «ф» (угловые минуты, ось ординат, при левом – график 2, и правом – график 3 - направлениях магнитоэллиптической модуляции +\- 225 угловых минут, а также линейной и обычной эллиптической поляризациях противоположных направлений +- 225 угловых минут – график 1) в зависимости от величины напряжённости импульсов магнитного поля основного соленоида Н2, модель магнитного поля Земли (в кЭ, ось абсцисс).

Блок-схема макета прибора для исследования солнечно-земных взаимодействий

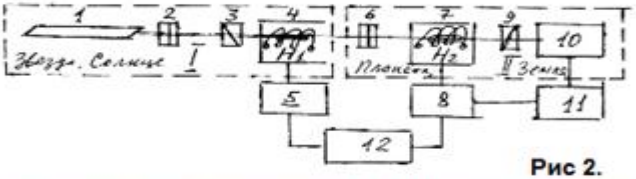

Рис 2.

1-ОКГ(оптич.квант.генератор), 2-ОК1(оптич.компенсатор), 3-поляризатор, 4-модулирующий имп.соленоид, 5-ГИТ1(генератор импульсов тока), 6-ОК2,7-основн. имп. соленоид, 8 –ГИТ2, 9-А (анализаор), 10-ФЭУ (фотоприемник), 11-источ. эл.питания, 12-блок управления.

Затем до оптического компенсатора проводилась магнитоэллиптическая модуляция (намагничивание по Фарадею) посредством магнитного вращения плоскости поляризации вправо или влево от нулевого положения на одинаковую величину (225+1) угл. минут при напряжённости магнитного поля Н1=5,71 кЭ в модулирующем соленоиде с кварцевым стеклом синхронно с импульсами магнитного поля основного соленоида Н2 линейно возрастающей напряжённости, в рабочем объёме которого находился исследуемый образец оргстекла. Тогда на выходе магнитооптической ячейки из Н1 и Н2 измерялись значительные и нелинейные изменения величин углов магнитного вращения большой оси магнитоэллиптически поляризованного излучения (рис. 1, график 2 для правой МЭП и график 3 для левой МЭЛ). Причём в области малых величин напряжённости импульсов магнитного поля основного соленоида (Н2<4,3кЭ) величина угла поворота большой оси магнитоэллипса поляризации нелинейно увеличивается и в несколько раз превышает величину обычного эффекта Фарадея при линейной или обычной эллиптической поляризации (рис. 1, график 1). Это может быть обусловлено несохранением углов пространственно-временной симметрии и самодействием микрочастиц [3**,** с. 238, 369, 837] вещества под влиянием магнитного поля, когда измеряемая величина угла поворота большой оси магнитоэллипса оказывается значительно увеличенной (более чем в 10 раз) даже при уменьшении напряжённости магнитного поля Н2 (рис., графики 2, 3) (Подобие LS – режима синергетики с обострением).

Для правой модулирующей магнитоэллиптической поляризации (график 2) измеряемые углы оказываются значительно больше, чем для левой МЭЛ (график 3) вплоть до напряженности 5,71 кЭ, когда измеряемые углы равны (232+1) для противоположных направлений модулирующей магнитоэллиптической поляризации. В последующем величина углов фарадеевского вращения магнитоэллиптически поляризованного излучения правого и левого знаков нелинейно уменьшается с увеличением напряженности Н2 импульсов магнитного поля, но уже измеряемые углы с левой МЭЛ- (график 3) по абсолютной величине больше, чем для правой МЭП+ (график 2) при напряженности магнитного поля Н2 >5,71кЭ (Подобие HS – режима синергетики).

Для моделирования солнечно-земных взаимодействий (рис. 2) измеренный поляризационно-магнитооптический эффект (рис.1, графики 2, 3) наиболее приемлем. Магнит 4 моделирует магнитное поле Солнца, а магнит 7 моделирует воздействие магнитного поля Земли.

Экспериментально обнаружен и измерен неизвестный ранее нелинейный поляризационно-магнитооптический эффект в сдвоенной

фарадеевской ячейке с оптическим компенсатором 6 между магнитами 4 (модулирующий) и 7 (основной), заключающийся в том, что при одинаковых величинах и противоположных по направлениям углов поворотов магнитоэллиптической модуляции 4 до ОК в исследуемом высокомолекулярном веществе из стабильных атомов в основном соленоиде 7 после ОК 6 измеряются нелинейные временные угловые структуры фарадеевского вращения (асимметричные, равносимметричные и антиасимметричные) при линейном изменении величин напряжённости магнитного поля 7 положительного направления, воздействующих на это вещество, которые даже увеличиваются с уменьшением напряжённости магнитного поля 7 (см. рис. 1). (В данных экспериментах также сохраняются все характеристики такого эффекта при ослаблении магнитооптического излучения в 10, 100 и 1000 раз нейтральными цветофильтрами).

С позиций физики и философии подобия [4, 5], а также физики как философии природы [6], блок-схема такого прибора (сдвоенная фарадеевская ячейка с оптическим компенсатором между магнитами 4 и 7) может быть физической моделью для исследования солнечно-земных взаимодействий (см. рис. 2).

В рабочем объёме импульсных соленоидов (с соответствующими металлическими экранами) число частиц исследуемых веществ вполне достаточно для самоорганизации. Изотропные, прозрачные, диамагнитные образцы имеют комнатную температуру и содержат стабильные, чётно-чётные атомные ядра кремния, кислорода, углерода, которые включают одинаковое число протонов «p» и нейтронов «n».

Магнитные поля воздействуют в первую очередь на процессы пространственного квантования спинов и на энергетические уровни любых микрочастиц всех иерархий в атомах, их ядрах, содержащих нуклоны с соответствующими кварками и глюонами. Все они задействованы в трёх фундаментальных взаимодействиях: сильном (радиус действия десять в минус тринадцатой степени сантиметра), слабом (радиус действия почти на три порядка меньше) и электромагнитном (дальнодействующее). Поэтому в магнитных полях происходит своеобразная пространственно-временная модуляция любого электромагнитного излучения (в том числе и лазерного) детерминированным квантовым хаосом в соленоиде модулятора (подобно поляризации магнитными полями пучков нейтронов). Такое излучение после своеобразного физического взаимодействия вследствие фундаментального двулучепреломления (разность хода между обыкновенным и необыкновенным лучами) в оптическом компенсаторе, синхронно поступает на исследуемое вещество в магнитном поле основного соленоида 7.

Сложнейшее информационное-физическое взаимодействие по причине изменчивости и становления в этом веществе двух детерминированных магнитными полями хаотических сигналов, как квантовых состояний, и образуют при самоорганизации в исследуемых веществах или в природе пространственно-временные физические структуры с прямо измеряемыми углами до (пространство – на входе ячейки) и после оптического компенсатора (время – на выходе этой ячейки). Такие чрезвычайные результаты проявления поляризационно-магнитооптических эффектов под воздействием двух магнитных полей также соответствуют теории физики квантовой информации [7] с учётом нелинейной динамики и квантовой запутанности [8].

Собственно, подобные физические структуры квантово-информационно управляют энергетическими процессами на микро, макро, глобальных и космических уровнях.

По современным теоретическим представлениям [9] закономерности природы, установленные в лабораторных экспериментах **остаются-верными-для-всей-Вселенной.** Исследуемые эффекты опубликованы также в журнале издания АН СССР [10].

Переходы линейных физических величин (магнитных полей, причина) в нелинейные угловые зависимости (следствие) в нелинейных динамических процессах спиновой динамики и синергетики, подтверждают также философскую проблему нарушений причинно-следственных связей в некоторых условиях, впервые исследованных Н.А. Козыревым [11]. Асимметрия времени, по мнению Н.А. Козырева, может представлять могучий источник энергии в «асимметричной механике, так как причинно-следственные изменения происходят не только во времени, но и с помощью времени», во взаимосвязи с пространственными структурами.

Открытые и измеренные мной нелинейные поляризационно-магнитооптические эффекты в определённой мере соответствуют основаниям физики, теоретически обоснованным Ю.С. Владимировым [12]. Им развивается новый подход к построению объединённой теории пространства-времени и физических взаимодействий (бинарной геометрофизики), которая опирается на понятия отношений между событиями.

12 марта 1832 года М. Фарадей [13] написал письмо для хранения в запечатанном виде в архивах Королевского Общества сроком на 100 лет, в котором особо отмечено: «… я хочу передать это письмо на хранение Королевскому Обществу, закрепить за собой определённой датой и таким образом иметь право, в случае экспериментального подтверждения, объявить эту дату датой моего открытия.»

Через 150 лет мной операционально открыты и измерены нелинейные поляризационно-магнитооптические эффекты нарушений магнитными полями величин угловых симметрий пространства-времени в стабильных атомах[14].

На основании вышеизложенного можно сформулировать отличительные признаки теоретической научной идеи М. Фарадея о переносе магнито-эллиптически поляризованным излучением (мерное физическое воздействие) от веществ из стабильных атомов в магнитном поле дальнодействущего нелинейного воздействия на любое вещество, находящееся в другом магнитном поле, и в этих веществах измеряются значительные по величине нелинейные нарушения величин угловых симметрий пространства-времени (различных структур) даже с обострением увеличивающихся при линейном уменьшении одного из магнитных полей, которые не изменяют своей формы и отличительных признаков при ослаблении магнитооптического излучения в 10, 100 и 1000 раз нейтральными светофильтрами.

Но все-таки основным в исследовании нелинейных нарушений угловых симметрий пространства-времени магнитными полями на моделях солнечно-земных взаимодействий оказывается принципиальная возможность перехода от глобальных процессов к микромасштабным, которые построены не на силовых или термодинамических процессах, а на *информационно-квантовых* взаимовлияниях фундаментальных взаимодействий (электромагнитных, сильных и слабых) с учётом спиновой динамики, но не броуновского движения для закрытых систем. Ещё в первой половине прошлого века академик В.Р. Вильямс [15] экспериментально доказал влияние рассеянного (всегда намагниченного по Фарадею [16, 17]) солнечного излучения на броуновское движение, а не движение молекул как таковых при комнатной температуре, то есть наблюдался явный антиэнтропийный процесс, как особо отметил П.Г. Кузнецов [18].

Предсказанные М. Фарадеем поляризационно-магнитооптические эффекты могут применяться при исследовании проблем влияния вариаций магнитного поля на перенос оптического излучения в земной атмосфере и в околоземном космическом пространстве [19]. Эффекты изменения свойств среды, сказывающихся на её оптических характеристиках при воздействии магнитного поля, обнаружены М.П. Чайкой в 1960-1970 гг. [20]. Под её руководством автор статьи выполнял в 1965 году выпускную дипломную работу по исследованию эффекта Фарадея некоторых диамагнитных веществ в униполярных импульсных магнитных полях.

Измеренные нелинейные поляризационно-магнитооптические

эффекты показывают, что в реальной природе энергетические процессы в атмосфере Земли детерминировано зависят не только от вариаций магнитных полей Земли, но и от их соотношения с величиной магнитного поля Солнца, а также от пространственной ориентации магнитных полей Солнца и Земли.

Литература

1. Хриплович И.Б. Несохранение чётности в атомных явлениях. – М.: Наука, 1981.

2. Бушье М.-А., Потье Л. Оптические эксперименты и слабые взаимодействия // Успехи физических наук. Т. 155, № 2, 1988. С. 299-310.

3. Физический энциклопедический словарь. – М., 1983, С. 238, 837.

4. Федосин С.П. Физика и философия подобия от преонов до метагалактик. Пермь, 1999.

5 Сиротенко Б.М. О подобиях микро- и макромира. – Л.: Гидрометеоиздат, 1990.

6. Захаров А.Д. Физика как философия природы. – М.: Наука, 2002.

7. Менский М.Б. Квантовые измерения и декогеренция. М.: Физматлит, 2004.

8. Доронин С.И. Квантовая магия. СПб.: Весь, 2007.

9. Чернуха В.В. Поляризационная теория Мироздания. – М.: Атомиздат, 2008. С. 37 п. Г2.

10. Ушаков И.И. Характеристики симметрии магнитно-поляризационных эффектов стеклообразного полиметилметакрилата // Высокомолекулярные соединения. 1989. Серия А, т. 31, №3. – С. 662-666.

11. Козырев Н.А. Избранные труды, Л.: ЛГУ, 1991.

12. Владимиров Ю.С. Геометрофизика. – М.: Бином, 2005.

13. Известия АН СССР, отделение техническое, № 5, 1938. С. 132.

14. Ушаков И.И. Поляризационно-магнитооптические методы исследования веществ // 6-ой Симпозиум по молекулярной спектроскопии высокого и сверхвысокого разрешения. Томск, Тезисы докладов, 15 – 17 сентября 1982. С. 236.

15. Вильямс В. Р. Собрание сочинений, том 1, Россельхозиздат, 1949. С. 151-152.

16. Фарадей М. Избранные труды по электричеству. – М.: ГОНТИ, 1939.

17. Фарадей М. Экспериментальные исследования по электричеству. Т. 1, 2, 3. Изд. АН СССР, 1947-1959.

18. Побиск Георгиевич Кузнецов Идеи и жизнь. – М.: Дубна 2000.

19. Мун Р., Кальво Ф., Гриднев К.А., Ивлев Л.С., Терехин Н.Ю., Васильев В.В. Лазерные исследования влияния вариаций напряженности магнитного поля на перенос излучения в атмосфере // Лазерные исследования в Санкт-Петербургском университете. Вып. 5, 2008. – С. 104-107.

20. Чайка М. П. Скрытые выстраивания возбужденных атомов при изотропном возбуждении. Оптика и спектроскопия, Т. 30, вып. 5, 1971. – С. 822-829.

О.Г. Юренков, канд. социол. наук,
доцент кафедры специальной техники
Санкт-Петербургского университета МВД России

Перспективы внедрения цифровых технологий в систему ведомственной связи МВД России

В настоящее время в системе органов внутренних дел России преобладает морально и физически устаревшая аналоговая техника радиосвязи. Такое положение дел приводит к невозможности реализации поставленных руководством страны задач по качественной модернизации всей правоохранительной системы. Между тем, внедрение современных систем связи, реализованных на базе цифровых технологий, может предоставить МВД России принципиально новые возможности по управлению подразделениями и обеспечению оперативно-служебной деятельности.

Перспективная система связи должна обеспечивать как минимум три основных режима: сетевой, режим прямой связи и режим ретрансляции. В сетевом режиме взаимодействие абонентов осуществляется с помощью базовых станций, которые распределяют каналы связи между абонентами. При условии реализации многостанционного доступа с частотным разделением каналов связи, сигналы управления передаются на отдельном, специально выделенном частотном канале. В режиме прямой связи обмен информацией между подвижными абонентами производится напрямую без участия базовой станции. В режиме ретрансляции связь между абонентами осуществляется через ретранслятор, который имеет фиксированные каналы передачи и приёма информации. Мобильные радиостанции должны обеспечивать возможность одновременного приёма информации как по каналам базовой станции (в сетевом режиме), так и по каналам прямой связи, от-

личным от сетевых. Такой режим работы радиосредств очень важен для оперативных подразделений. Он позволяет организовать взаимодействие между собой расположенных в пределах радиовидимости абонентов одного подразделения на каналах прямой связи с максимальной оперативностью. При этом сохраняется возможность получения старшим группы команд и директив от начальника подразделения, расположенного на значительном расстоянии от группы, через инфраструктуру базовых станций.

Системе связи необходимо обеспечить передачу в сетях связи, как речевой информации, так и различного типа данных. Службы речевой связи должны устанавливать различные виды соединений: циркулярную связь с широковещательным вызовом, групповое и индивидуальное соединения, которые могут производиться с помощью стандартного или аварийного вызовов, а также с помощью множественного вызова с использованием списка абонентов. Важнейшим способом организации связи между абонентами, ориентированным, прежде всего, на использование оперативными службами, для которых чрезвычайно важно установление группового соединения с минимальной задержкой, является многоместный открытый канал. При данном способе определённые ресурсы сети связи по команде от диспетчера сети или привилегированного пользователя закрепляются за некоторой группой абонентов. После установления открытого канала групповое соединение производится без обмена информацией по каналу управления, что позволяет существенно сократить время установления соединения.

Служба передачи данных должна обеспечивать ряд услуг прикладного уровня, поддерживаемых заложенными в радиотерминалах функциями, таких, как межабонентский обмен сообщениями, доступ к централизованным базам данных, доступ к фиксированным сетям, передача факсимильных сообщений, пересылка файлов, передача сигналов персонального вызова, передача коротких сообщений, передача статусных вызовов, поддержка режима передачи получаемых с помощью приёмников систем спутниковой навигации данных о местоположении объекта, передача потока видеоизображений.

Важна и функция избирательного прослушивания, которая позволяет несанкционированному для данного вызова пользователю прослушивать разговор. Как правило, такая возможность должна предоставляться диспетчеру сети. При прослушивании диспетчер может либо вступить в разговор, либо прекратить ведение разговора. Данная функция позволяет диспетчеру сети следить за ходом конкретной операции, проводимой с использованием радиосредств, и при необходи-

мости самостоятельно давать необходимые указания или команды.

Безусловно, полезной является служба дистанционного прослушивания, которая обеспечивает возможность включения по определённой команде абонентской станции в режим передачи без разрешения на это её пользователя. Данный режим может применяться для акустического прослушивания обстановки у конкретного абонента в определённой ситуации. Так, например, может прослушиваться салон служебного автомобиля при получении сведений о нападении на автомашину.

Указанные выше и ещё многие существенные возможности реализуемы только на основе внедрения цифровых технологий, что повлечёт за собой практически полное переоснащение имеющегося в МВД России парка средств связи.

Под общей редакцией начальника кафедры
специальных информационных систем
кандидата юридических наук, доцента
Кабанова Андрея Александровича
e-mail: *akabanov @ inbox.ru*

Правовая информатика

Материалы выступлений на заседании 20 секции
30 международной конференции
«Школьная информатика и проблемы устойчивого развития»
в Санкт-Петербургском университете МВД России
23 апреля 2011 г.

Составитель: А.А. Кабанов

Печатается в авторской редакции

Подписано в печать и свет 13.04.2011 Тираж 100 экз.
Объём 6,25 печ. л. Формат 60×84/16 Печать офсетная. Не для продажи.

Отпечатано в ООО «Копи-Р Групп»
190000, Санкт-Петербург, пер. Гривцова, д. 1/64