В.А. Мазуров, В.В.Невинский

Понятие и принципы информационной безопасности

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений [1, с. 4].

Стремительный рост компьютеризации основных сфер человеческой деятельности, охватывающий управление государством, вооруженными силами, работой ядерных реакторов, химических заводов, финансово-банковскую деятельность, изучение космоса и подобное, с одной стороны, позволил обеспечить высокие достижения в области науки, техники, культуры, управления и организации жизнедеятельности общества в целом. С другой стороны, наличие глобальных компьютерных сетей и недостаточная их защищенность от сбоев техники, вызванных самыми различными причинами, от неправомерных действий людей, совершенных умышленно или по неосторожности, могут вызвать самые непредсказуемые вредные для человека и общества последствия.

Новые технологии порождают и новые преступления. Согласно унификации Комитета министров Европейского Совета определены криминальные направления компьютерной деятельности. К ним относятся: *компьютерное мошенничество,* которое является причиной экономических потерь государственных, частных организаций и граждан; *подделка компьютерной информации* – традиционные методы изменения содержания документов с использованием современных информационных технологий; повреждение данных или программ, обрабатывающихся или хранящихся в компьютерных базах данных; *компьютерный саботаж* – ввод, изменение, стирание, модификация, фальсификация данных или программ; *несанкционированный доступ* к информации, нарушающий установленные правила получения информации; *несанкционированный перехват данных; несанкционированное использование защищенных компьютерных программ* – воспроизведение, распространение и эксплуатация программного продукта, который защищен правами автора в соответствии с Законом об авторском праве.

Преступления в информационной сфере наносят большой материальный и моральный вред. Так, по данным зарубежной правоохранительной практики, например, в Германии с использованием компьютеров похищается до 4 млрд марок ежегодно, во Франции – до 1 млрд франков, в США – до нескольких миллиардов долларов [2, с. 5]. Институтом компьютерной безопасности США отмечалось, что резко возрастает число обращений в правоохранительные органы по поводу компьютерных преступлений, 30% респондентов из них сообщали, что их информационные системы были взломаны внешними злоумышленниками. Атакам через Интернет подвергались 57% опрошенных, 55% отметили нарушения со стороны собственных сотрудников.

По данным ГИЦ МВД РФ в 1997 г. было зарегистрировано 7 преступлений в сфере компьютерной информации, в 1998 г. – 66, в 1999 г. – 294 и в первом квартале 2002 г. – 865 преступлений.

В последнее время в России вышло достаточно большое количество публикаций, посвященных вопросам обеспечения компьютерной безопасности, однако имеют место неоднозначные суждения, выводы и предложения по совершенствованию этой деятельности. Отдельные теоретические положения, в том числе и относительно понятия «информационная безопасность», имеют различные толкования.

Актуальность данноой проблемы заключается:

– в особом характере общественной опасности преступных посягательств на информационную безопасность;

– наличии тенденций к росту числа преступлений в информационной сфере;

– неразработанности ряда теоретических положений, связанных с информационной безопасностью;

– необходимости осуществления объективно обусловленной интеграции технических и юридических наук в данной сфере общественных отношений.

За последнее десятилетие в России реализован комплекс мер по совершенствованию обеспечения информационной безопасности. Для правового обеспечения информационной безопасности приняты Федеральные законы «О государственной тайне», «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О правовой охране программ для ЭВМ и баз данных», Основы законодательства РФ об Архивном фонде Российской Федерации и архивах, а также ряд других нормативных актов. В новых Гражданском и Уголовном кодексах предусмотрена ответственность за правонарушения и преступления в информационной сфере [3–7].

Процесс формирования базы правового обеспечения информационной безопасности продолжается и в настоящее время, что объясняется определенными качественными изменениями отношений в информационной сфере. Так, в декабре 2002 г. принят ФЗ «О внесении изменений и дополнений в Закон РФ «О правовой охране программ для ЭВМ и баз данных» [8], на рассмотрении в Государственной Думе находятся законопроекты «О коммерческой тайне», «Об информации персонального характера». Назрела необходимость разработки и принятия законов «О служебной тайне», «О профессиональной тайне». Принятие указанных законов обусловлено положениями Доктрины информационной безопасности РФ, в которой в качестве основных составляющих национальных интересов России в информационной сфере выделяются меры правового характера, обеспечивающие конституционные права человека и гражданина свободно искать, передавать, производить и распространять информацию любым законным способом, конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем [1].

В Доктрине дается определение информационной безопасности. *Под информационной безопасностью Российской Федерации* понимается *состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства* [1, с. 4].

В юридической литературе отмечаются неоднозначные подходы к определению понятия информационной безопасности. Так, по мнению М.В. Арсентьева, информационная безопасность – снятие информационной неопределенности относительно объективно и субъективно существующих реальных и потенциальных угроз за счет контроля над мировым информационным пространством и наличие возможностей, условий и средств для отражения этих угроз, что в совокупности определяет уровень (степень) информационной безопасности каждого субъекта [9, с. 50].

В.Ю. Статьев и В.А. Тиньков определяют информационную безопасность как защиту информации и поддерживающей ее инфраструктуры с помощью совокупности программных, аппаратно-программных средств и методов с целью недопущения причинения вреда владельцам этой информации или поддерживающей его инфраструктуре [10, с. 68].

По мнению Г.Г. Феоктистова, информационная безопасность – это получение максимальной информации о намерениях и потенциальных действиях своих оппонентов и минимальная утечка информации о своих планах. Она включает в себя комплекс мер и совокупность действий, направленных на защиту собственных источников информации, каналов ее передачи и создание систем дезинформации [11, с. 211–212].

А.Д. Урсул определяет информационную безопасность как состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям [12, с. 7].

Указанные определения, на наш взгляд, имеют некоторые недостатки. С одной стороны, дается широкое, неконкретизированное определение информационной безопасности, требующее дополнительного толкования и конкретизации, с другой стороны, не учтены отдельные аспекты обеспечения информационной безопасности, вместе с тем рассмотренные определения несут важную смысловую нагрузку и основополагающие положения относительно рассматриваемого понятия. Прежде всего указываются объект защиты, конкретная деятельность по обеспечению защищенности информации.

На наш взгляд, определение информационной безопасности необходимо сформулировать на основе действующего законодательства, Доктрины информационной безопасности Российской Федерации, которая представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопас-

ности Российской Федерации, развивает Концепцию национальной безопасности Российской Федерации применительно к информационной сфере.

В указанных источниках сформулированы понятия «информация», «информационная сфера», «безопасность». Информация – это сведения о лицах, предметах, фактах, событиях и процессах. На сегодняшний день в научно-правовой литературе выделяется более двадцати видов информации по ее отраслевой принадлежности и востребованности в обществе (правовая, научная, финансовая, банковская, коммерческая, медицинская и т.д.). Нет объективной необходимости обеспечивать защиту буквально всей информации. Принято подразделять информацию на открытую и ограниченного доступа. Для эффективного решения задач защиты информации целесообразно в качестве объекта защиты избрать информацию ограниченного доступа. На наш взгляд, данную информацию можно подразделить на конфиденциальную информацию (сведения) и государственную тайну. Конфиденциальная информация – доверительная, не подлежащая огласке информация, доступ к которой ограничивается в соответствии с законодательством. Конфиденциальность информации определяет и доверяет посторонним лицам владелец этой информации. В отличие от конфиденциальной информации государственная тайна определяется государством через соответствующие государственные органы, получение и разглашение этой информации строго регламентировано нормативными актами, информация имеет гриф секретности [13].

К конфиденциальной информации относятся сведения, составляющие тайну частной жизни, профессиональную, служебную, коммерческую тайну [14]. *Тайна частной жизни* – это охраняемые законом конфиденциальные сведения, составляющие личную и семейную тайну лица, незаконное собирание или распространение которых причиняет вред правам и законным интересам этого лица и предоставляет ему право на защиту в соответствии с законодательством Российской Федерации.

Профессиональная тайна – это охраняемые законом конфиденциальные сведения, доверенные или ставшие известными лицу исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, незаконное получение или распространение которых может повлечь за собой вред правам и законным интересам другого лица, доверившего эти сведения, и привлечение к ответственности в соответствии с действующим законодательством.

Служебная тайна – это охраняемая законом конфиденциальная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости, а также ставшая известной в государственных органах и органах местного самоуправления только на законном основании и в силу исполнения их представителями служебных обязанностей, имеющая действительную или потенциальную ценность в силу неизвестности ее третьим лицам.

Коммерческая тайна – это охраняемые законом конфиденциальные сведения в области производственно-хозяйственной, управленческой, финансовой деятельности организации, имеющие действительную или потенциальную ценность в силу неизвестности их третьим лицам, к ним нет свободного доступа на законном основании, обладатель сведений принимает меры к их конфиденциальности, незаконное получение, использование или разглашение которых создает угрозу причинения вреда владельцу этих сведений и предоставляет ему право на возмещение причиненных убытков или уголовно-правовую защиту в соответствии с законодательством Российской Федерации.

В отличие от рассмотренных выше охраняемых законом видов тайн, содержание государственной тайны находит свое законодательное закрепление в Законе РФ «О государственной тайне» [4]. *Государственная тайна* – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Указанные в данном определении сведения конкретизированы в Перечне сведений, относящихся к государственной тайне [13].

Ответственность за посягательство на указанные виды тайны предусмотрена в Уголовном кодексе РФ (ст. 137, 138, 142, 155, 183, 275, 276, 283, 284, 310, 311, 320). В УК РФ 1996 г. включена новая, не известная прежнему уголовному законодательству России, глава 28 «Преступления в сфере компьютерной информации» (ст. 272, 273, 274). Указанные нормы уголовного закона входят в систему правовых мер, направленных на защиту информации, прав и законных интересов граждан, общества и государства в информационной сфере.

Право на информацию складывается из двух элементов – права на получение информации

и права на ее распространение. Первое относится не к гражданским, частным, а к публичным правам. Право же на передачу информации имеет гражданско-правовое содержание, оно представляет собой исключительное право [15, с. 27]. Законом РФ «О правовой охране программ для ЭВМ и баз данных» регулируются отношения, возникающие в связи с правовой охраной и использованием программ для ЭВМ и баз данных. В ст. 12 данного закона права на программу для ЭВМ или базу данных отнесены к исключительным правам владельца информации [7].

В содержание *информационной безопасности* входит информационная сфера. Определение информационной сферы сформулировано в ФЗ «Об участии в международном информационном обмене». *Информационная сфера* (среда) – сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации [6].

В основе понятия «информационная безопасность» лежит понятие «безопасность», которое нашло свое отражение в Законе РФ «О безопасности». *Безопасность* – это состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз. К *жизненно важным интересам* закон относит совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства. Основные *объекты безопасности*: личность, ее права и свободы; общество, его материальные и духовные ценности; государство, его конституционный строй, суверенитет и территориальная целостность [16].

Таким образом, *информационная безопасность* – состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере от внешних и внутренних угроз, обеспечивающее ее формирование, использование и развитие.

Под *защищенностью* понимается совокупность правовых, научно-технических, специальных, организационных мер, направленных на своевременное выявление, предупреждение и пресечение неправомерного получения и распространения защищаемой информации, осуществляемых органами законодательной, исполнительной и судебной власти, общественными и иными организациями и объединениями, гражданами, принимающими участие в обеспечении информационной безопасности в соответствии с законодательством, регламентирующим отношения в информационной сфере.

Правовые меры – деятельность законодательных органов по созданию правовой базы, обеспечивающей надлежащее формирование, распространение и использование информации; регулирующей деятельность субъектов, осуществляющих создание, преобразование и потребление информации; предусматривающей ответственность за нарушения в информационной сфере, меры обеспечения безопасности и правовой защиты информации, информационной инфраструктуры.

Научно-технические меры – деятельность субъектов, осуществляющих свою работу в информационной сфере, направленная на своевременное и активное использование достижений научно-технического прогресса в обеспечении информационной безопасности, а также участие в разработке новых технологий, программ, научно обоснованных способов защиты информации.

Специальные меры – деятельность государственных органов, уполномоченных осуществлять разведывательные, контрразведывательные, оперативно-розыскные мероприятия, направленные на упреждающее получение информации о планах, намерениях, устремлениях специальных служб, информационных и иных организаций, конкурентов и частных лиц, с использованием специальных технических средств, иных источников информации, указанных в Федеральном законе «Об оперативно-розыскной деятельности», в целях предупреждения и пресечения утечки защищаемой информации, выявление и привлечение к ответственности виновных лиц, а также получения информации о новых разработках, технологиях, средствах и способах формирования, обработки и использования информационных ресурсов для практического внедрения в собственную деятельность по обеспечению информационной безопасности [17].

Организационные меры – деятельность субъектов по обеспечению физической, технической защиты информации, оборудования и носителей информации. Разработка и внедрение программ информационной безопасности и контроль за их выполнением, взаимодействие и обмен опытом защиты информации с правоохранительными, информационными органами. Работа по подбору, допуску и проверке персонала, подготовка и обучение сотрудников приемам работы с охраняемой информацией и ее носителями.

Одним из важнейших аспектов информационной безопасности является определение и классификация возможных угроз безопасности.

Угроза безопасности – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства. В Законе РФ «О безопасности» и Доктрине информационной безопасности РФ угрозы подразделяются на внешние и внутренние.

К *внешним источникам угроз* информационной безопасности РФ относятся: деятельность иностранных разведывательных и информационных структур, международных террористических организаций, а также обострение международной конкуренции за обладание информационными технологиями и ресурсами; увеличение технологического отрыва ведущих государств мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий.

К *внутренним источникам угроз* относятся: критическое состояние отечественных отраслей промышленности; неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере; недостаточная координация деятельности федеральных органов власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной безопасности РФ; недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика; низкое финансирование мероприятий по обеспечению информационной безопасности; отставание России от ведущих стран мира по уровню информатизации в жизненно важных сферах государственной деятельности и ряд других источников угроз [16].

В литературе выделяются различные классификации угроз безопасности автоматизированным информационным системам [18, с. 5–13]. Среди них можно выделить следующие:

По источнику угрозы:

– *внешние* – связанные со стихийными бедствиями, техногенными, политическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями;

– *внутренние* – связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения.

По природе возникновения:

– *естественные (объективные)* – вызванные воздействием на информационную среду объективных физических процессов или стихийных природных явлений, не зависящих от воли человека;

– *искусственные (субъективные)* – вызванные воздействием на информационную сферу человека. Среди искусственных угроз выделяют:

а) непреднамеренные (случайные) угрозы – ошибки программного обеспечения, персонала, отказы вычислительной и коммуникационной техники и т.д.;

б) преднамеренные (умышленные) угрозы – неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ и т.д. Преднамеренные угрозы обусловлены действиями людей и ориентированы на неправомерное нарушение конфиденциальности, целостности и доступности информации, а также использование ресурсов в своих целях.

По принципу воздействия: с использованием доступа; с использованием скрытых каналов.

По цели реализации: нарушение а) конфиденциальности; б) целостности; в) доступности.

По характеру воздействия: активные; пассивные.

По объекту воздействия: угрозы, воздействующие а) на информационную среду в целом; б) на ее отдельные элементы.

Кроме этого, в литературе имеет место классификация основных угроз по степени их опасности: несанкционированный доступ; пожары; умышленное нарушение нормальной работы (заражение вирусами, умышленный ввод искаженных данных, умышленный вывод из строя оборудования и его хищения); использование программного обеспечения, содержащего ошибки [19, с. 70].

Основные проблемы информационной безопасности связаны прежде всего с умышленными угрозами (действиями людей), так как они являются основной причиной и движущей силой преступлений и правонарушений. В то же время средства вычислительной техники (прежде всего ЭВМ), встраиваясь в систему отношений по поддержанию информационной безопасности, оказывают на них определенное воздействие. В отдельных случаях ЭВМ функционируют как источники повышенной опасности, и тогда нарушение установленных правил

их эксплуатации может привести к нарушению информационной безопасности.

Деятельность по обеспечению информационной безопасности строится на основе определенных принципов. В Законе РФ «О безопасности» сформулированы основные принципы обеспечения безопасности. К ним относятся: законность; соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства по обеспечению безопасности; интеграция с международными системами безопасности [16].

Законность – в широком смысле принцип точного и неукоснительного исполнения всеми органами государства, должностными лицами и гражданами требований закона. Законность – это один из элементов демократии и правового государства. Принцип законности служит базой для законотворчества в части правового обеспечения защиты информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, системы регулирования возникающих при этом отношений, требует, чтобы содержание всех законов соответствовало положениям Конституции РФ, международным договорам и соглашениям России с зарубежными государствами, заключенными для координации и взаимодействия в вопросах противодействия преступным посягательствам в информационной сфере. Правоохранительные, иные государственные органы, частные организации и граждане, уполномоченные осуществлять деятельность по обеспечению информационной безопасности, обязаны точно и неукоснительно соблюдать требования действующего законодательства. Виновные в совершении правонарушений и преступлений в информационной сфере несут ответственность в соответствии с действующим административным, гражданским и уголовным законом.

Применительно к информационной безопасности, на наш взгляд, можно выделить принципы обоснованности, своевременности и прогноза.

Принцип обоснованности. Защите подлежит прежде всего информация ограниченного доступа, т.е. информация, незаконное получение и распространение которой может причинить вред гражданину, обществу и государству. Необоснованная защита информации, прежде всего ограничение доступа к ней, посягает на конституционные права граждан на информацию, а в отдельных случаях препятствует развитию экономики, научно-технического прогресса, отношений в жизненно важных областях деятельности общества и государства. Принцип обоснованности заключается в установлении путем экспертной оценки целесообразности ограничения доступа к конкретной информации, выделении вероятных экономических и иных последствий этого акта исходя из баланса жизненно важных интересов личности, общества, государства, разработки адекватных мер противодействия внешним и внутренним угрозам информационной безопасности.

Принцип своевременности защиты информационной сферы позволяет реализовать процедуру предварительного ограничения доступа к защищаемой информации, осуществлять ее защиту и заключается в установлении ограничений на распространение этой информации с момента ее получения, разработки или заблаговременно. Значение этого принципа заключается прежде всего в том, что ограничение доступа к защищаемой информации, информационным системам, если не исключает полностью, то делает маловероятной возможность совершения преступных посягательств в данной сфере. На практике своевременность достигается путем разработки и четкого исполнения положений концепции и системы защиты объекта, на котором сконцентрированы технические средства, средства связи, информация, подлежащая защите. Система защиты включает в себя совокупность правовых, научно-технических, специальных и организационных мер. Особое значение данного принципа проявляется в тех случаях, когда та или иная тема, проект, исследование находятся на стадии разработки, изучения, анализа, и при этом разработчики не уделяют должного внимания ограничению доступа к результатам работы, используют незащищенные каналы и средства связи, ЭВМ, привлекают к работе непроверенных специалистов и т.д. Как известно, новые разработки, направления исследований, технологии представляют повышенный интерес и являются приоритетным направлением в деятельности разведывательных органов иностранных государств, промышленного шпионажа, конкурентов, преступных элементов.

Принцип прогноза информационной безопасности заключается в выделении конкретных внешних и внутренних угроз к охраняемой информационной сфере и базируется на объективной, реальной оценке охраняемых объектов – информации, инфраструктуры, субъектов, связанных с созданием, преобразованием и по-

треблением информации; моделировании возможной противоправной деятельности, посягающей на информационную безопасность. Прогноз осуществляется на основе уже имеющихся материалов о работе российских и зарубежных правоохранительных органов по выявлению, предупреждению и пресечению противоправной деятельности в информационной сфере, изучения и анализа практики защиты информации, информационной инфраструктуры, а также путем активного применения достижений науки и техники, особенно в области модернизации и совершенствования возможностей ЭВМ. Значение данного принципа заключается в том, что создается вероятность осуществлять мероприятия по обеспечению информационной безопасности в упреждающем режиме и за счет этого снизить потери, ущерб от преступных устремлений противников, конкурентов, преступников.

В заключение можно отметить, что информационная безопасность в современных условиях приобретает все большую актуальность и значимость, является одним из приоритетных направлений обеспечения национальной безопасности России, а также международной безопасности, что требует теоретического осмысления основных положений информационной безопасности для совершенствования правовой базы и правоприменительной практики. Одному из аспектов этой проблемы и посвящена данная статья.

Литература

1. Доктрина информационной безопасности РФ // Российская газета. 2000. 28 сент.

2. Панфилова Е.П. Компьютерные преступления / Под общ. ред. Б.В. Волженкина. М., 1999.

3. Уголовный кодекс РФ. М., 2001.

4. О государственной тайне: Закон РФ от 21 июля 1993 г. // Закон. 1999. №2.

5. Об информации, информатизации и защите информации: Федеральный закон от 20 февраля 1995 г. // СЗ РФ. 1995. №8.

6. Об участии в международном информационном обмене: Федеральный закон от 4 июня 1996 г. // СЗ РФ. 1996. №28.

7. О правовой охране программ для ЭВМ и баз данных: Закон РФ от 23 сентября 1992 г. // СЗ РФ. 1992. №42.

8. О внесении изменений и дополнений в Закон РФ «О правовой охране программ для ЭВМ и баз данных»: Федеральный закон от 24 декабря 2002 г. // Российская газета. 2002. 28 дек.

9. Арсентьев М.В. К вопросу о понятии «информационная безопасность» // Информационное общество. 1997. №4–6.

10. Статьев В.Ю., Тиньков В.А. Информационная безопасность распределенных информационных систем // Информационное общество. 1997. №1.

11. Феоктистов Г.Г. Информационная безопасность общества // Социально-политический журнал. 1996. №5.

12. Урсул А.Д. Информационная стратегия и безопасность в концепции устойчивого развития // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 1996. №1.

13. О Перечне сведений, отнесенных к государственной тайне: Указ Президента РФ №61 от 24 января 1998 г. // Российская газета. 1998. 3 февр.

14. О Перечне сведений конфиденциального характера: Указ Президента РФ №188 от 6 марта 1997 г. // Закон. 1998. №2.

15. Дозорцев В.А. Информация как объект исключительного права //Дело и Право. 1996. №4.

16. О безопасности: Закон РФ от 5 марта 1992 г. // Ведомости съезда народных депутатов РФ и Верховного Совета РФ. 1992. №15.

17. Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. // СЗ. 1995. №33.

18. Охрименко С.А., Черней Г.А. Угрозы безопасности автоматизированным информационным системам (программные злоупотребления) // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 1996. №5.

19. Герасименко В.Г., Сергеев В.В. Информационная безопасность в банках США и Великобритании // Банковское дело. 1996. №7.