На правах рукописи

Величко Михаил Юрьевич

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ: ТЕОРЕТИКО-ПРАВОВОЙ АСПЕКТ

Специальность 12.00.01 – теория и история права и государства; история учений о праве и государстве

Автореферат диссертации на соискание ученой степени кандидата юридических наук

Казань - 2007

Работа выполнена на кафедре теории и истории государства и права Государственного образовательного учреждения высшего профессионального образования «Казанский государственный университет им. В.И. Ульянова-Ленина»

Научный руководитель
доктор юридических наук, профессор
Горбачев Иван Георгиевич

Официальные оппоненты:
заслуженный юрист РФ, доктор юридических наук, профессор
Александров Алексей Иванович

доктор юридических наук, профессор
Медведев Валентин Григорьевич

Ведущая организация
Государственное образовательное учреждение высшего профессионального образования «Московский университет МВД России»

Защита диссертации состоится 20 сентября 2007 года в 14 часов на заседании Диссертационного совета К 212.081.01 по защите диссертаций на соискание ученой степени кандидата юридических наук при Государственном образовательном учреждении высшего профессионального образования «Казанский государственный университет им. В.И. Ульянова-Ленина» (420008, г. Казань, ул. Кремлевская, д.18, ауд.324).

С диссертацией можно ознакомиться в научной библиотеке им. Н.И. Лобачевского Государственного образовательного учреждения высшего профессионального образования «Казанский государственный университет им. В.И. Ульянова-Ленина».

Автореферат разослан 17 августа 2007г.

Ученый секретарь
диссертационного совета
кандидат юридических наук, доцент  Г.Р. Хабибуллина

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. В результате осуществления социально-экономических преобразований за истекшие годы общество и общественные отношения в России перешли в качественно новое состояние, характеризующееся, в частности, сильным сращиванием органов власти, организаций бизнеса и криминалитета, что диктует острую потребность пересмотра функций и задач правоохранительных органов, органов обеспечения национальной безопасности, сил обеспечения экономической безопасности и правопорядка.

Переход в новое состояние российского общества неразрывно связан с возникновением новых вызовов и угроз как национальной безопасности в целом, так и ее важнейших составляющих - экономической и общественной безопасности. Возникновение указанных угроз на фоне сильного отставания и недостаточного развития российской законодательной основы сопряжено, прежде всего, с ускоренной капитализацией экономических отношений общества, бурным развитием рыночных отношений, тесным встраиванием России в глобальные мировые экономические отношения, глобализацией мировой экономики, глобализацией и транснационализацией преступности в основных жизненно важных сферах общественных отношений, возникновением и развитием международного терроризма и др.

Все это требует серьезного осмысления и выработки новых механизмов организации противодействия национальной и транснациональной преступности.

Необходимым условием социально-экономического развития Российской Федерации является снижение уровня преступности. Существующее состояние, применяемые правоохранительные механизмы и средства борьбы с современной преступностью не в полной мере соответствуют состоянию и динамике распространения организованной преступности, теневой экономике и экономической преступности, наркоторговле и торговле людьми, терроризму и экстремизму, коррупции.

Информационная революция способствует созданию и включению в социально-экономическую систему таких потоков информации, которые могут быть вполне достаточными для эффективного разрешения большинства современных глобальных и региональных социально-экономических проблем, для обеспечения рационального природопользования, гармоничного экономического, политического, социального и культурно-духовного развития общества и его безопасности. Этими же достижениями в сфере информации в полной мере пользуется и преступность, которая в своей основе является масштабной и организованной, охватывая целые регионы и даже всю территорию страны, выходя за ее пределы, имеет большие возможности по доступу к информационным, техническим и финансовым ресурсам, их наращиванию и использованию в своей противоправной деятельности. Указанные обстоятельства обусловливают необходимость кардинального переосмысления существующих взглядов и выработки новых концептуальных подходов к проблеме информационной безопасности, борьбы с такими новыми явлениями как киберпреступность и кибертерроризм в целях обеспечения национальной безопасности.

Актуальность исследования правовых и организационно-управленческих механизмов обеспечения информационной безопасности органов внутренних дел в условиях интеграции информационных систем правоохранительных органов и специальных служб обусловлена также тем, что вопросы теории защиты информации традиционно рассматривались, как правило, с технических позиций или применительно к ранее существующим и устоявшимся организационным системам.

В ряде исследований отмечается, что проблему обеспечения защиты информации часто сужают до проблемы обеспечения защиты только компьютерной информации. Так, О.В. Генне справедливо полагает, что для

реализации эффективного подхода необходимо взаимоувязанное рассмотрение ряда аспектов информационной безопасности[1].

Формирование режима информационной безопасности - проблема комплексная, в которой можно выделить четыре уровня: *законодательный* (законы, нормативные акты, стандарты и т.п.); *административный* (действия общего характера, предпринимаемые руководством); *процедурный* (меры безопасности, направленные на контроль за соблюдением сотрудниками мер, направленных на обеспечение информационной безопасности); *программно-технический* (технические меры).

Исходя из этого, возникает необходимость развития теоретических положений и методологических принципов обеспечения информационной безопасности органами внутренних дел. Особую значимость приобретает научно-практическая проблема комплексного рассмотрения вопросов государственно-правового регулирования и организационного управления в сфере обеспечения информационной безопасности правоохранительных органов. Все это определило актуальность темы исследования и рассматриваемый круг вопросов.

Состояние изученности проблемы. Вопросы государственного регулирования в информационной сфере в значительной мере стали затрагиваться в научных публикациях лишь во второй половине XX века, когда форсированными темпами стал развиваться международный обмен научно-техническими достижениями. Большой вклад в рассматриваемую область внесли следующие отечественные ученые: В.Д. Аносов, А.Б. Антопольский, Г.Т. Артамонов, П.И. Асяев, Ю.М. Батурин, И.Л. Бачило, М. Боер, А.Б. Венгеров, М.И. Дзлиев, Г.В. Емельянов, И.Ф. Исмагилов, В.А. Копылов, В.А. Лебедев, В.Н. Лопатин, Г.Г. Почепцов, М.М. Рассолов, И.М. Рассолов, А.А. Стрельцов, А.Д. Урсул, А.А. Фатьянов, А.П. Фисун и др. Среди зарубежных

[1] См.: Генне О.В. Основные положения стеганографии // Защита информации Конфидент. - 2000. - №3. – С.20-25.

ученых в данном направлении можно отметить работы Р. Голдшейдера, И. Джерарда, Дж. Майера, Б. Маркуса, Дж. Ромари, С. Филипса и др.

Цель и задачи диссертационного исследования. Целью исследования является уточнение теоретико-правовых положений, методологических принципов обеспечения информационной безопасности органов внутренних дел, информационного противоборства и эффективного информационного противодействия криминальным структурам с применением правовых и правоохранительных механизмов.

В соответствии с сформулированной целью в работе были поставлены следующие **задачи**:

- исследовать и уточнить теоретические и методологические основы государственно-правового регулирования в сфере защиты информации и организации информационной безопасности органов внутренних дел;

- определить пути совершенствования правовых механизмов защиты информации, организационные мероприятия и управленческие решения по борьбе с компьютерными преступлениями;

- выявить роль правовых и организационных механизмов защиты информации в системах информационного обеспечения деятельности органов внутренних дел;

- разработать предложения по формированию организационно-правовых механизмов обеспечения информационной безопасности органов внутренних дел.

Объектом диссертационного исследования выступает информационная безопасность органов внутренних дел.

Предметом исследования являются правовые и организационно-управленческие механизмы обеспечения информационной безопасности органов внутренних дел.

Теоретико-методологической основой диссертационного исследования послужили теоретические и методологические разработки

отечественных и зарубежных ученых по проблемам национальной, экономической и информационной безопасности, защите информации.

В основу исследования положена системная методология, разработанная В.Н. Анищенко, Б.В. Ахлибининским, Л.Б. Баженовым, Р.Н. Байгузиным, Б.В. Бирюковым, В.В. Бордюже, В.В. Вержбицким, Г.Г. Вдовиченко, В.А. Галатенко, А.П. Герасимовым, И.И. Гришкиным, Д.И. Дубровским, Н.И. Жуковым, А.М. Коршуновым, К.Е. Морозовым, И.Б. Новик, Л.А. Петрушенко, М.И. Сетровым, А.Д. Урсул, Г.И. Царегородцевым и др.

Теоретико-правовой основой диссертационного исследования стали труды ученых в области уголовного права, криминологии, теории права информатики, среди которых работы: С.С. Алексеева, Ю.М. Батурина, Н.И. Ветрова, В.Б. Вехова, Б.В. Здравомыслова, В.В. Крылова, В.Н. Кудрявцева, Ю.И. Ляпунова, А.В. Наумова, С.А. Пашина, А.А. Пионтковского, Н.А. Селиванова, А.Н. Трайнина, О.Ф. Шишова.

При проведении исследования применялись диалектический, формально-юридический, сравнительно-правовой, абстрактно-логический, аналитический и системный методы, а также метод экспертных оценок; широко использовались методы прикладных, специальных дисциплин (уголовного права, статистики, информатики, теории информационной безопасности).

Нормативно-правовой основой исследования послужили положения международного законодательства, правовой базы Российской Федерации по защите информации, Уголовный кодекс Российской Федерации и основанные на них нормативные правовые документы.

Научная новизна диссертационного исследования определяется комплексным анализом правовых и организационных механизмов обеспечения информационной безопасности органов внутренних дел.

Научная новизна исследования заключается в самой постановке проблемы и выборе круга рассматриваемых вопросов. Настоящая диссертация является первой в отечественной юридической науке работой, посвященной комплексному исследованию правовых и организационных основ

информационной безопасности правоохранительных органов Российской Федерации, основу которых образуют органы внутренних дел МВД России. В ней впервые проанализированы современные угрозы национальной безопасности в информационной сфере, исходящие от организованной национальной и транснациональной преступности, коррупции, терроризма, экстремизма и криминальной экономики, обоснованы роль и место информационной безопасности в общей системе обеспечения национальной безопасности. Впервые выполнен комплексный анализ целей, задач, функций и полномочий органов внутренних дел в сфере борьбы с компьютерными преступлениями и кибернетическим терроризмом, обеспечения информационной безопасности в оперативно-служебной деятельности. На основе взаимоувязанной оценки состояния оперативной обстановки и характера преступлений в информационной сфере, масштабов, форм, методов и средств информационного противодействия правоохранительным органам со стороны преступности, обосновано положение о нахождении органов внутренних дел в состоянии информационной войны с различными видами преступности, прежде всего, организованной и экономической. Сформулированы предложения по направлениям совершенствования государственно-правового регулирования отношений в области обеспечения информационной безопасности органов внутренних дел и развитию действующего законодательства.

Практическая значимость результатов диссертационного исследования заключается в их направленности на решение задач, стоящих перед органами внутренних дел по обеспечению законности и правопорядка, безопасности государства, общества и личности.

Полученные в ходе исследования теоретические положения, сформулированные выводы и практические рекомендации могут способствовать проведению согласованной государственной политики в области обеспечения национальной и информационной безопасности, поэтапному совершенствованию государственно-правового регулирования

отношений органов внутренних дел в сфере защиты информации, противодействия компьютерной преступности и кибернетическому терроризму.

Выводы и рекомендации соискателя использовались при обосновании государственно-правовых мер и механизмов обеспечения информационной безопасности органов внутренних дел, подготовке докладов руководству МВД России и в высшие органы исполнительной власти Российской Федерации по вопросам обеспечения безопасности.

Теоретические разработки соискателя могут послужить основой дальнейших научных изысканий в области обеспечения национальной безопасности российского государства и общества, а также могут быть использованы в образовательном процессе высших учебных заведений и научно-исследовательских учреждений МВД России.

Положения, выносимые на защиту. В процессе исследования получен ряд новых теоретических положений, которые выносятся на защиту:

- В современных условиях информационная безопасность общества, государства и личности является, наряду с другими видами безопасности, включая экономическую, важнейшей составляющей национальной безопасности.

Угрозы информационной безопасности страны, источниками которых являются современные национальные и транснациональные преступные сообщества, по своей совокупности и масштабам воздействия охватывая всю территорию страны и затрагивая все сферы жизнедеятельности общества, подрывают основы национальной безопасности Российской Федерации, нанося ей значительный ущерб.

- Органы внутренних дел МВД России являются важной составляющей сил и средств противодействия информационным посягательствам криминальных сообществ на права и свободы граждан, безопасность государства, общества и личности.

В условиях современного состояния преступности, которая в своей основе является масштабной и организованной, охватывает целые регионы и

даже всю территорию страны, выходя за ее пределы, имеет большие возможности по доступу к информационным средствам и оружию, их наращиванию и использованию в своей противоправной деятельности, невозможно обеспечить информационную безопасность органов внутренних дел только на основе применения защитных средств и механизмов. В этих условиях необходимо вести активные наступательные (боевые) действия с использованием всех видов информационного оружия и других наступательных средств в целях обеспечения превосходства над преступностью в информационной сфере.

- Органы внутренних дел МВД России находятся в состоянии информационной войны как с национальными, так и транснациональными преступными сообществами, специфическим содержанием и основной формой ведения которой являются информационная борьба с использованием информационно-вычислительных и радиосредств, средств радиотехнической разведки, информационно-телекоммуникационных систем, включая каналы космической связи, геоинформационных систем и иных информационных систем, комплексов и средств.

- На эволюции правового режима, организационных основ и собственно деятельности органов внутренних дел по обеспечению информационной безопасности, противодействию компьютерным преступлениям и кибернетическому терроризму сильно отразились изменения в политическом и социально-экономическом положении страны. Выработанные и реализуемые подходы к «силовому» обеспечению правопорядка и безопасности в условиях высокой активности организованных криминальных сообществ требуют кардинального переосмысления существующих взглядов и выработки новых концептуальных подходов к проблеме государственно-правового регулирования отношений в сфере информационной безопасности, борьбы с такими новыми явлениями как кибернетическая преступность и кибернетический терроризм в целях обеспечения национальной безопасности.

• Общесоциальный характер деятельности органов внутренних дел, необходимость четкой правовой регламентации их деятельности в особых условиях ведения информационной войны с масштабной организованной преступностью требуют создания соответствующего государственно-правового режима и отражения его в основополагающих политических и нормативных правовых документах. Поэтому логически обоснованным представляется дополнение Концепции национальной безопасности и Доктрины информационной безопасности Российской Федерации, закона РСФСР «О безопасности» положениями относительно понятия «информационная война» и условий применения информационного оружия в борьбе с кибернетической преступностью и кибернетическим терроризмом, а также расширение круга правомочий сотрудников органов внутренних дел в законе РСФСР «О милиции» в части особых условий применения информационного оружия в целях эффективного противодействия организованной преступности при возникновении прямых угроз информационной безопасности общества и государства.

Апробация результатов диссертационного исследования. Ряд положений настоящей работы обсуждались на научно-практической конференции «Институциональные, экономические и юридические основы финансовых расследований в борьбе с терроризмом» (Академия экономической безопасности МВД России, 2006), межведомственном круглом столе «Актуальные проблемы законодательного регулирования оперативно-розыскной деятельности органов охраны правопорядка» и межведомственной научной конференции «Актуальные вопросы теории и практики оперативно-розыскной деятельности органов внутренних дел по борьбе с экономическими преступлениями», Всероссийской научно-практической конференции «Противодействие легализации преступных доходов: проблемы и пути их решения» (Академия экономической безопасности МВД России и Всероссийский научно-исследовательский институт МВД России, 2007). Материал диссертационного исследования использован при подготовке

специализированных лекций по проблемам ответственности за совершение преступлений в сфере компьютерной информации на курсах повышения квалификации органов по борьбе с экономическими преступлениями.

Основные положения и выводы диссертации изложены в шести научных публикациях.

Объем и структура диссертационного исследования. Структура и объем диссертации определяются целью и задачами исследования. Она состоит из введения, трех глав, объединяющих восемь параграфов, заключения и списка использованной литературы.

II. ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во Введении обосновывается актуальность избранной темы, раскрывается степень ее научной разработанности, определяются объект, предмет, цель и задачи исследования, формулируются основные положения, выносимые на защиту, обосновываются теоретическая и методологическая основы, раскрываются научная новизна и практическая значимость исследования, приводятся сведения об апробации его результатов.

Глава I. Теоретико-правовые основы информационной безопасности

Глава первая посвящена исследованию и теоретическому осмыслению категории «информационная безопасность», а также юридической природы указанного явления, принципов, образующих собой содержание информационной безопасности, которая является самостоятельной областью исследования.

Первый параграф - *«Информационная безопасность в системе национальной безопасности: природа, сущность, место в категориальном аппарате общей теории права»* - представляет собой общетеоретическое правовое обоснование концепции информационной безопасности.

Сущность информационной безопасности раскрыта в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 9 сентября 2000 г. № Пр-1895. Под информационной безопасностью понимается состояние защищенности национальных интересов в информационной сфере, которые определяются совокупностью сбалансированных интересов личности, общества и государства.

Доктрина информационной безопасности Российской Федерации развивает Концепцию национальной безопасности Российской Федерации, утвержденную Указом Президента Российской Федерации от 17 декабря 1997 г. №1300 (в ред. Указа Президента РФ от 10 января 2000 г. №24), применительно к информационной сфере. В Концепции национальной безопасности отмечено, что важнейшими задачами обеспечения информационной безопасности Российской Федерации являются:

- реализация конституционных прав и свобод граждан Российской Федерации в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;
- противодействие угрозе развязывания противоборства в информационной сфере.

Значимость обеспечения информационной безопасности государства можно продемонстрировать любыми примерами негативного характера, наблюдаемыми в процессе деформации российской экономики, достаточно лишь указать на дефолт 1998 г. Решение задач обеспечения безопасности борьбы в информационной сфере не сводится только к защите каналов и средств передачи информации, охране государственной тайны, правительственной связи, информации и другим вопросам, которые принято рассматривать при анализе совокупности угроз и системы мер по обеспечению информационной безопасности. К вопросам информационной безопасности в экономической сфере также относится безопасность информационных систем

управления промышленностью, отраслями (включая оборонный комплекс), предприятиями, банками.

В современных условиях угрозу национальной безопасности представляют информационные технологии, появилось новое направление в науке - информационная безопасность. Влияние угроз в информационной сфере во все возрастающей степени направленно на интересы личности, общества и государства. При этом воздействие на личность с целью снижения активности жизненной позиции проводится посредством средств и технологий коммуникаций. Нарастает информационное воздействие на экономическую систему, включая финансовую сферу (например, информационные атаки против национальных валют и фондовых рынков, прокатившиеся по миру в конце 1990-х годов), фондовые рынки с игрой на понижение капитализации предприятий, а затем их скупкой по более низкой цене в сочетании с распространением информации по созданию негативного образа конкурента и т.д.

Особую опасность представляют информационные угрозы государству через распространение и внедрение идеологии международного терроризма и сепаратизма.

Во втором параграфе - *«Организационно-правовые основы обеспечения информационной безопасности»* - дается анализ организационных решений, регламентированных в нормативных правовых актах, так или иначе регулирующих сферу обеспечения информационной безопасности личности, общества и государства.

Организационно-правовое обеспечение информационной безопасности представляет собою совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению информационной безопасности, так и создание, функционирование систем защиты информации на конкретных объектах. Основными функциями организационно-правового обеспечения являются: разработка основных принципов отнесения сведений, имеющих конфиденциальный характер, к

защищаемой информации; определение системы органов и должностных лиц, ответственных за обеспечение информационной безопасности в стране, и порядка регулирования деятельности предприятия и организации в этой области; создание полного комплекса нормативно-правовых руководящих и методических материалов (документов), регламентирующих вопросы обеспечения информационной безопасности как в стране в целом, так и на конкретном объекте; определение мер ответственности за нарушения правил защиты и порядка разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Под юридическими аспектами организационно-правового обеспечения защиты информации понимается совокупность законов и других нормативных правовых актов, с помощью которых достигались бы следующие цели: все правила защиты информации являются обязательными для соблюдения всеми лицами, имеющими отношение к конфиденциальной информации; узакониваются все меры ответственности за нарушение правил защиты информации; узакониваются (приобретают юридическую силу) технико-математические решения вопросов организационно-правового обеспечения защиты информации, а также узакониваются процессуальные процедуры разрешения ситуаций, складывающихся в процессе функционирования системы защиты.

Разработка законодательной базы информационной безопасности любого государства является необходимой мерой, удовлетворяющей первейшую потребность в защите информации при определении социально-экономических, политических, военных направлений развития этого государства. Особое внимание со стороны западных стран к формированию такой базы вызвано все увеличивающимися затратами на борьбу с «информационными» преступлениями, что заставляет их серьезно заниматься вопросами законодательства по защите информации. Так, первый закон в этой области в США был принят в 1906 г., а к настоящему времени уже имеется более 500 законодательных актов по защите информации, ответственности за ее разглашение и компьютерные преступления.

Правовое обеспечение защиты информации в Российской Федерации разрабатывается по трем направлениям: защита прав личности на частную жизнь, защита государственных интересов и защита предпринимательской и финансовой деятельности.

Структура нормативной базы по вопросам информационной безопасности Российской Федерации включает: Конституцию Российской Федерации, конституционные федеральные законы, федеральные законы, постановления Правительства Российской Федерации; ведомственные нормативные акты, ГОСТы, руководящие документы. Среди федеральных законов можно выделить: «О государственной тайне», «О безопасности», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных», «Об участии в международном информационном обмене», «О связи», «О коммерческой тайне» и др.

Глава II. Угрозы информационной безопасности в деятельности органов внутренних дел

Во второй главе анализируются факторы, условия и явления, которые являются или могут быть источниками угроз информационной безопасности в деятельности органов внутренних дел.

Первый параграф - *«Компьютерная и телекоммуникационная преступность»* - посвящен исследованию механизмов преступного воздействия на технические и программные средства информатизации, а также прогнозированию и оценке криминальных ситуаций.

Развитие информационных и телекоммуникационных технологий привело к тому, что современное общество в огромной мере зависит от управления различными процессами посредством компьютерной техники, электронной обработки, хранения, доступа и передачи информации. Согласно информации Бюро специальных технических мероприятий МВД России, в прошлом году было зафиксировано более 14 тыс. преступлений, связанных с

высокими технологиями, что немного выше, чем в позапрошлом году. Анализ складывающейся ситуации показывает, что около 16% злоумышленников, действующих в «компьютерной» сфере криминала, - это молодые люди в возрасте до 18 лет, 58% - от 18 до 25 лет, причем около 70% из них имеют высшее либо незаконченное высшее образование.

Проведенные исследования показали, что 52% установленных правонарушителей имели специальную подготовку в области информационных технологий, 97% были сотрудниками государственных учреждений и организаций, использующими ЭВМ и информационные технологии в своей повседневной деятельности, 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

По неофициальным экспертным оценкам, из 100% возбуждаемых уголовных дел около 30% доходят до суда и только 10-15% подсудимых отбывают наказание в тюрьме. Большинство дел переквалифицируются или прекращаются за недостаточностью улик. Реальное положение дел по странам СНГ – вопрос из области фантастики. Компьютерные преступления относятся к преступлениям с высокой латентностью, отображающей существование в стране той реальной ситуации, когда определенная часть преступности остается неучтенной.

Во втором параграфе - *«Информационный терроризм: понятие, правовая квалификация, средства противодействия»* - проводится теоретико-правовой анализ категории «информационный терроризм», определяются угрозы и методы кибернетического терроризма.

Серьезную опасность для всего мирового сообщества представляет все более распространяющийся технологический терроризм, составной частью которого является информационный или кибернетический терроризм.

Мишенями террористов становятся компьютеры и созданные на их основе специализированные системы - банковские, биржевые, архивные, исследовательские, управленческие, а также средства коммуникации - от

спутников непосредственного телевещания и связи до радиотелефонов и пейджеров.

Методы информационного терроризма совершенно иные, нежели традиционного: не физическое уничтожение людей (или его угроза) и ликвидация материальных ценностей, не разрушение важных стратегических и экономических объектов, а широкомасштабное нарушение работы финансовых и коммуникационных сетей и систем, частичное разрушение экономической инфраструктуры и навязывание властным структурам своей воли.

Опасность информационного терроризма неизмеримо возрастает в условиях глобализации, когда средства телекоммуникаций приобретают исключительную роль.

В условиях кибернетического терроризма возможная модель террористического воздействия будет иметь «трехступенчатый» вид: первая ступень - это выдвижение политических требований с угрозой в случае их невыполнения парализовать всю экономическую систему страны (во всяком случае, ту ее часть, которая использует в работе компьютерные технологии), вторая - произвести демонстрационную атаку на информационные ресурсы достаточно крупной экономической структуры и парализовать ее действие, а третья - повторить требования в более жесткой форме, опираясь на эффект демонстрации силы.

Отличительной чертой информационного терроризма является его дешевизна и сложность обнаружения. Система Internet, связавшая компьютерные сети по всей планете, изменила правила, касающиеся современного оружия. Анонимность, обеспечиваемая Internetom, позволяет террористу стать невидимым, как следствие, практически неуязвимым и ничем (в первую очередь жизнью) не рискующим при проведении преступной акции.

Положение усугубляется тем, что преступления в информационной сфере, в число которых входит и кибернетический терроризм, влекут за собой наказание существенно меньшее, чем за осуществление «традиционных» террористических актов. В соответствии с Уголовным кодексом РФ (ст. 273),

создание программ для ЭВМ или внесение изменений в существующие программы, которые заведомо приводят 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 наказывается лишением свободы на срок максимум до семи лет. Для сравнения, в США законы карают несанкционированное проникновение в компьютерные сети заключением сроком до 20 лет.

Основой обеспечения эффективной борьбы с кибернетическим терроризмом является создание эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению такого рода деятельности. Для борьбы с терроризмом во всех его проявлениях работают различные антитеррористические органы. Особое внимание борьбе с терроризмом уделяют развитые страны мира, считая его едва ли не главной опасностью для общества.

В третьем параграфе - *«Информационная война: организационно-правовое обеспечение государственного противодействия кибернетической преступности»* - рассматривается понятие, природа, средства ведения информационной войны и пути обеспечения эффективного информационного противодействия преступности.

Угрозы информационной безопасности страны, источниками которых являются современная преступность, преступные национальные и транснациональные сообщества, по своей совокупности и масштабам воздействия охватывающие всю территорию страны и затрагивающие все сферы жизнедеятельности общества, обусловливают необходимость рассмотрения борьбы между организованной преступностью и призванными ей противостоять правоохранительными органами, прежде всего, органами внутренних дел, как информационную войну, основной формой ведения которой и ее специфическим содержанием являются информационная борьба с использованием информационно-вычислительных и радиосредств, средств

радиотехнической разведки, информационно-телекоммуникационных систем, включая каналы космической связи, геоинформационных систем и иных информационных систем, комплексов и средств.

В условиях современного состояния преступности обеспечить информационную безопасность в деятельности органов внутренних дел невозможно только на основе применения защитных средств и механизмов. В этих условиях необходимо вести активные наступательные (боевые) действия с использованием всех видов информационного оружия и других наступательных средств в целях обеспечения превосходства над преступностью в информационной сфере.

Появление и развитие новых масштабных явлений в жизни страны и общества, новых угроз национальной безопасности со стороны преступного мира, в распоряжении которого находится современное информационное оружие, и новых условий осуществления оперативно-служебной деятельности органов внутренних дел, определяемых потребностями ведения информационной войны с национальной и транснациональной в своей основе организованной преступностью, обусловливают необходимость соответствующего законодательного, государственно-правового регулирования отношений в сфере информационной безопасности государства в целом и органов внутренних дел в частности.

В целях создания необходимой правовой основы эффективного осуществления правоохранительной деятельности в условиях информационной войны с преступным миром предлагается, в частности:

- расширить круг правомочий сотрудников органов внутренних дел в Законе Российской Федерации «О милиции» в части особых условий применения информационного оружия в целях эффективного противодействия организованной преступности при возникновении прямых угроз информационной безопасности общества и государства, а также дополнить Концепцию национальной безопасности Российской Федерации и Доктрину информационной безопасности Российской Федерации положением

относительно понятия и условий применения информационного оружия в борьбе с кибернетической преступностью и кибернетическим терроризмом.

Глава III. Основные направления совершенствования нормативно-правового и организационного обеспечения информационной безопасности в деятельности органов внутренних дел

Третья глава посвящена определению путей дальнейшего совершенствования нормативно-правового регулирования и организационно-управленческого обеспечения информационной безопасности в деятельности органов внутренних дел.

В первом параграфе - *«Государственно-правовое регулирование в сфере борьбы с компьютерными преступлениями»* - определяются меры пассивного и активного противодействия кибернетической преступности.

К основным мероприятиям государственно-правового характера по обеспечению информационной безопасности, осуществляемым, в том числе, и органами внутренних дел, предлагается отнести: формирование режима и охраны в целях исключения возможности тайного проникновения на территорию размещения информационных ресурсов; определение методов работы с сотрудниками при подборе и расстановке персонала; проведение работы с документами и документированной информацией, включая разработку и использование документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение; определение порядка использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации; создание технологии анализа внутренних и внешних угроз конфиденциальной информации и выработки мер по обеспечению ее защиты; осуществление систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Анализ действующего российского законодательства в области информационной безопасности и государственной системы защиты

информации позволяет выделить важнейшие полномочия органов внутренних дел в сфере обеспечения информационной безопасности государства: отражение информационной агрессии, направленной против страны, комплексная защита информационных ресурсов, а также информационно-телекоммуникационной структуры государства; недопущение и разрешение международных конфликтов и инцидентов в информационной сфере; предупреждение и пресечение преступлений и административных правонарушений в информационной сфере; защита иных важных интересов личности, общества и государства от внешних и внутренних угроз.

Во втором параграфе - *«Совершенствование нормативно-правовой базы по защите информации органов внутренних дел»* - определены направления и пути совершенствования законодательства по защите информации органов внутренних дел.

Правовая защита информации, как ресурса, признана на международном и государственном уровнях. На международном уровне она определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном же уровне правовая защита регулируется государственными и ведомственными актами.

К основным направлениям развития российского законодательства в целях защиты информации органов внутренних дел целесообразно отнести:

- законодательное закрепление механизма отнесения объектов информационной инфраструктуры органов внутренних дел к критически важным и обеспечение их информационной безопасности, включая разработку и принятие требований к техническим и программным средствам, используемым в информационной инфраструктуре этих объектов;
- совершенствование законодательства об оперативно-розыскной деятельности в части создания необходимых условий для проведения оперативно-розыскных мероприятий в целях выявления, предупреждения, пресечения и раскрытия компьютерных преступлений и преступлений в сфере высоких технологий; усиления контроля за сбором, хранением и

использованием органами внутренних дел информации о частной жизни граждан, сведений, составляющих личную, семейную, служебную и коммерческую тайны; уточнения состава оперативно-розыскных мероприятий;

- усиление ответственности за преступления в сфере компьютерной информации и уточнение составов преступлений с учетом Европейской конвенции о кибернетической преступности;
- совершенствование уголовно-процессуального законодательства в целях создания условий для правоохранительных органов, обеспечивающих организацию и осуществление оперативного и эффективного противодействия преступности, осуществляемого с использованием информационно-телекоммуникационных технологий для получения необходимых доказательств.

В третьем параграфе - *«Организационно-управленческий и правовой механизм защиты информации в деятельности органов внутренних дел: пути дальнейшего развития»* - рассматриваются основные направления совершенствования организационного и правового аспектов защиты информации в деятельности органов внутренних дел.

Организационно-управленческие меры являются решающим звеном формирования и реализации комплексной защиты информации в деятельности органов внутренних дел.

При обработке или хранении информации органам внутренних дел в рамках защиты от несанкционированного доступа рекомендуется проведение следующих организационных мероприятий: выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите; определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено; установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам защиты; ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей

документацией, определяющей требования и порядок обработки конфиденциальной информации; получение от объекта доступа расписки о неразглашении доверенной ему конфиденциальной информации.

В соответствии с Законом Российской Федерации «О милиции», к компетенции МВД России отнесены функции по формированию общегосударственных справочно-информационных фондов оперативного и криминалистического учета. Выполнение этих функций осуществляется информационными и техническими подразделениями служб МВД России во взаимодействии с подразделениями криминальной милиции, милиции общественной безопасности, пенитенциарными учреждениями, другими правоохранительными органами, правительственными учреждениями и организациями, ведающими вопросами общественной безопасности, а также правоохранительными органами (полицией) иных государств.

Информационное взаимодействие в сфере борьбы с преступностью ведется в рамках законов Российской Федерации «Об оперативно-розыскной деятельности», «О безопасности», «Об учетах и учетной деятельности в правоохранительных органах», действующих уголовного и уголовно-процессуального законодательства, международных соглашений МВД России в сфере обмена информацией, Положения о МВД России, приказов Министра внутренних дел России.

Исследования показали, что концептуальные положения обеспечения информационной безопасности правоохранительных органов должны включать требования к переходу к единой нормативно-правовой базе, регулирующей процессы использования информации в борьбе с преступностью. При этом в системе министерства внутренних дел вместо многочисленной группы ведомственных актов предлагается ввести три группы нормативно-правовых документов по информационному обеспечению: отраслевые, общего пользования; отраслевые, по линиям служб; нормативно-правовую документацию местного уровня управления по локальным прикладным

проблемам информационного обеспечения территориального органа внутренних дел.

В **Заключении** исследования излагаются основные выводы и обозначаются пути дальнейшего совершенствования механизма обеспечения информационной безопасности в деятельности органов внутренних дел.

По теме диссертации опубликованы следующие работы:

Работы, опубликованные в изданиях, рецензируемых ВАК:

1. Величко М.Ю. Актуальные проблемы борьбы с киберпреступностью: правовые аспекты / М.Ю. Величко // Юридический мир. - 2007. - № 8. – С.87-93 (0,4 п.л.).

Работы, опубликованные в иных изданиях:

2. Величко М.Ю. Информационная безопасность в деятельности органов внутренних дел: Науч. изд. / М.Ю. Величко. - М.: Изд-во ИНИОН РАН, 2007. – 130 с. (8,125 п.л.).

3. Величко М.Ю. Организационное обеспечение информационной безопасности в деятельности органов внутренних дел (теоретико-правовой аспект) / М.Ю. Величко // Противодействие легализации преступных доходов: Сб. науч. трудов. - М.: РИО АЭБ МВД России, 2007. – С.132-136 (0,275 п.л.).

4. Величко М.Ю. Компьютерные преступления в интернет / М.Ю. Величко // Актуальные вопросы теории и практики оперативно-розыскной деятельности органов внутренних дел по борьбе с экономическими преступлениями: Сб. науч. трудов. - М.: РИО АЭБ МВД России, 2007. – С.220-226 (0,4 п.л.).

5. Величко М.Ю. Информационный терроризм / М.Ю. Величко // Институциональные, экономические и юридические основы финансовых

расследований в борьбе с терроризмом: Сб. науч. трудов. - М.: РИО АЭБ МВД России, 2006. – С.205-218 (0,8 п.л.).

6. Величко М.Ю. Возможные угрозы экономической безопасности при информатизации общества / М.Ю. Величко // Проблемы обеспечения экономической безопасности, противодействия теневой экономике и подрыва экономических основ терроризма: Сб. науч. докл. – М.: РИО АЭБ МВД России, 2005. – С.192-199 (0,45 п.л.).