На правах рукописи

ЛОПАТИНА ТАТЬЯНА МИХАЙЛОВНА

КРИМИНОЛОГИЧЕСКИЕ И УГОЛОВНО-ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Специальность 12.00.08 – уголовное право и криминология; уголовно-исполнительное право

Автореферат
диссертации на соискание ученой степени доктора
юридических наук

Москва - 2006

Диссертация выполнена в Государственном учреждении «Всероссийский научно-исследовательский институт Министерства внутренних дел Российской Федерации».

Научный консультант - Заслуженный деятель науки Российской Федерации, доктор юридических наук, профессор Антонян Юрий Миранович.

Официальные оппоненты - доктор юридических наук, профессор Гладких Виктор Иванович;

доктор юридических наук, профессор Чучаев Александр Иванович;

доктор юридических наук, профессор Трунцевский Юрий Владимирович.

Ведущая организация - Академия права и управления Федеральной службы исполнения наказаний России.

Защита диссертации состоится «14» ноября 2006 г. в 14.00 часов на заседании диссертационного совета по присуждению ученой степени доктора юридических наук Д 203.005.02 при Государственном учреждении «Всероссийский научно-исследовательский институт Министерства внутренних дел Российской Федерации (123995, г. Москва, ул. Поварская, 25).

С диссертацией можно ознакомиться в библиотеке ВНИИ МВД России.

Автореферат разослан « 7 » июля 2006 г.

Ученый секретарь
диссертационного совета Кулешов Р. В.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. Актуальность диссертационного исследования определяется рядом обстоятельств, характеризующих важность, масштабность и многогранность проблемы.

Первое обстоятельство обусловлено социальной значимостью правопорядка, стержнем которого является, с одной стороны, неуклонное соблюдение и исполнение правовых норм всеми гражданами, государственными органами, предприятиями, организациями и учреждениями и, с другой – фактически обеспечиваемая возможность беспрепятственной реализации конституционных прав, свобод и законных интересов граждан, а также интересов в целом общества и государства. Современная информационная сфера обусловливает возникновение принципиально нового вида прав – информационных, ставших объектом уголовно-правовой охраны. Тенденция активного внедрения информационных технологий во все сферы жизни и деятельности человека, наряду с позитивными завоеваниями, «обогатила» криминальную практику новым видом преступлений – в сфере компьютерной информации.

История последних десятилетий свидетельствует о прогрессирующем, по сравнению с другими видами преступных посягательств, росте преступлений с использованием ЭВМ. Во-первых, они приносят лицам, их совершившим, колоссальные прибыли при сравнительно легком доступе к финансовым средствам. Во-вторых, организованные преступные группы и сообщества стали придавать приоритетное значение получению конфиденциальной информации о деятельности государственных органов и коммерческих структур для реализации своих преступных замыслов и обеспечения собственной безопасности. В-третьих, компьютерная преступность связана с множеством факторов, имеющих социально-правовое значение для всего мирового сообщества. В условиях нарастающей глобализации

информационная сфера становится не только ареной международного сотрудничества, но и полем противодействия, о чем свидетельствует потенциальный рост активности международного терроризма. Подтверждением этого являются статистические данные Совета безопасности Российской Федерации, согласно которым в 2004 г. выявлено более 800 тыс. попыток осуществления компьютерных атак на официальные информационные ресурсы органов государственной власти, при этом более 69 тыс. из них – на официальное Internet-представительство Президента России.

Второе обстоятельство заключается в том, что российская информационная сфера отличается несовершенством правовых отношений. В силу этого пользователи, с одной стороны, не могут не балансировать "на грани фола", поскольку далеко не всегда имеются четкие юридические ориентиры правомерного поведения участников информационного процесса. Такое положение обусловливает высокую степень криминологической уязвимости информационной сферы для недобросовестных участников информационных отношений. С другой, информационная сфера не может развиваться сбалансировано, поскольку пользователи не всегда «вооружены» организационно-правовыми и техническими мерами безопасности. Это обусловливает неэффективность предупредительных мер в процессе создания безопасных условий информационного обмена. Государство, общество, коммерческие и финансовые учреждения, отдельные граждане нуждаются в защите от криминальных посягательств в сфере компьютерной информации.

Разработка соответствующих методов защиты должна вестись на основе постоянного и целенаправленного изучения криминологических особенностей преступных проявлений нового типа, а также лиц, их совершающих, и компьютерной среды, способной создавать ранее неизвестные условия для совершения противоправных действий и концентрации лиц с криминальной направленностью. А это, в свою

очередь, актуализирует необходимость контроля за происходящими процессами со стороны правоохранительных органов, проблемы противодействия компьютерным преступлениям и обеспечения компьютерной безопасности, которая представляет собой одну из сторон использования информационных технологий.

Статистика свидетельствует, что компьютерная техника все чаще выступает орудием совершения преступлений. По некоторым данным, в России общий ущерб, нанесенный преступными посягательствами только в сфере электронных платежей, – около 6 млрд. долларов в год[1]. Для сравнения: в США ущерб от компьютерных преступлений составляет ежегодно 5 млрд. долларов, во Франции – около 1 млрд. евро при ежегодном увеличении числа подобных преступлений на 30–40%, в Германии при помощи компьютеров похищается порядка 4 млрд. евро[2].

Усложнение и нарастание преступной деятельности с использованием возможностей компьютерных технологий имеет тенденцию к устойчивому росту, и нет достаточных оснований считать, что в ближайшее время ситуация может измениться в лучшую сторону. Положение усугубляется тем, что компьютерные преступления совершаются новым типом преступника – интеллектуальным и предприимчивым, использующим «изощренные» в техническим отношении способы преступной деятельности. Диапазон преступников весьма широк: от молодых людей до высококвалифицированных, респектабельных специалистов, занимающих высокое социальное положение.

Третье обстоятельство состоит в трудностях применения уголовно-правовых норм в следственной и судебной практике. Эти трудности

---

[1] Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – С. 7.

[2] Анин Б. Защита компьютерной информации. – СПб.: БХВ – Санкт-Петербург, 2000. – С. 7.

многообразны и связаны, в частности, с казуистичностью формулировок диспозиций отдельных норм преступлений в сфере компьютерной информации; их бланкетностью; влиянием норм других отраслей российского законодательства на применение указанных уголовно-правовых норм и т. д. В связи с чем практика их официального толкования требует усовершенствования.

Четвертое обстоятельство выражается в том, что в теории отечественного уголовного права исследованы и разрешены не все аспекты проблемы ответственности за преступления в сфере компьютерной информации; не определено понятие компьютерного преступления; круг норм об ответственности за компьютерные преступления с учетом соответствующего международного законодательства нуждается в дополнении и т. д. В криминологии только накапливается теоретико-правовой опыт противодействия преступным деяниям, связанным с противоправным использованием компьютерной техники и информационных технологий.

Указанные основополагающие обстоятельства с достаточной, по нашему представлению, убедительностью обосновывают принципиальное значение анализа отечественной практики предупреждения преступлений в сфере компьютерной информации, опосредование положительного мирового опыта сквозь призму национальных особенностей развития российского общества, актуальность проблем ответственности за компьютерные преступления, её важность и необходимость исследования на диссертационном уровне.

Степень научной разработанности темы. Научное изучение и практическое решение проблем компьютерной преступности в Российской Федерации представляет известную сложность в силу своей многоаспектности и предполагает научную проработку отдельных теоретико-методологических вопросов, определение основных

направлений, форм и методов практической реализации полученного знания.

Общенаучные проблемы, связанные с процессами компьютеризации общества, рассматривались в трудах А. И. Анчишкина, П. Г. Бунича, Н. Н. Моисеева, А. М. Яковлева и других. Место, роль и значение компьютеризации – в трудах М. С. Вертузаева, Э. П. Вечернина, В. И. Майорова, В. П. Полежаева, С. Ю. Яковлева и других ученых. Влияние компьютеризации на политическую, культурную, научно-познавательную сферы – в трудах В. Н. Бусленко, Г. Г. Воробьева, А. Г. Здравомыслова, Г. Б. Кочеткова, В. М. Николайчука, В. Пкелиса, В. К. Португала, А. И. Ракитова, А. П. Суханова, А. Д. Урсула.

Значительный вклад в изучение проблем компьютеризации внесли зарубежные ученые: Дж. Бэмфорд, Дж. А. Гарриери, Дж. П. Грант, Г. Каг, О. Э. Лейста, Ж. Л. Лорьер, Кр. Дж. Мак-Кланг, Поль А. Страссман, Б. Холыст, Ф. Фукуяма.

В качестве теоретико-методологической базы исследований общественных процессов, которые связаны с использованием телекоммуникационных, биоэлектронных и психокомпьютерных технологий, могут служить работы С. С. Алексеева, В. С. Афанасьева, И. Л. Бачило, О. А. Гаврилина, Н. Л. Гранат, В. М. Горшенева, И. А. Ильина, В. П. Казимирчука, Д. А. Керимова, Ю. Н. Колосова, В. Н. Кудрявцева, В. В. Лазарева, Р. З. Лившица, Г. В. Мальцева, Н. И. Матузова, М. Н. Марченко, Н. Н. Моисеева, А. С. Пиголкина, С. В. Полениной, В. П. Сальникова, В. А. Шабалина, Л. С. Явича и других.

Вопросы уголовно-правовой оценки компьютерных преступлений освещались в трудах таких ученых, как В. М. Аверьянов, Ю. М. Батурин, А. М. Жодзишский, А. В. Венгеров, В. В. Вехов, В. В. Крылов, В. Д. Курушин, Ю. И. Ляпунов, В. Ю. Максимов, В. А. Минаев, И. В. Никифоров, А. С. Попов, Н. А. Селиванов, А. Б. Тельба, Д. Файков, А. С. Черных и других; криминалистические и отдельные криминологические

аспекты – в работах Д. Айкова, Б. Е. Богданова, Р. С. Белкина, А. В. Гортинского, С. П. Голубятникова, А. Н. Караханьяна, В. Е. Козлова, В. В. Крылова, Г. Н. Мухина, Н. С. Полевого, С. Г. Спириной, С. П. Фортинского, В. Н. Черкасова, Н. Г. Шурухнова и других ученых.

Не преуменьшая роли исследований уголовно-правовых и криминалистических вопросов, полагаем, что не менее важное значение имеет разработка криминологических аспектов компьютерной преступности. В настоящее время кардинально изменились социально-экономические условия в обществе, обострилась криминогенная ситуация, значительные нововведения претерпело уголовное законодательство. Все это настоятельно диктует необходимость осмысления современных аспектов компьютерной преступности и ее основных угроз, причем не только с теоретико-правовых позиций или уголовно-правовой защиты компьютерной информации, но и под углом зрения криминологической науки, формирования в рамках общей криминологии нового научного направления – *компьютерной криминологии.*

Объект и предмет исследования. *Объект* исследования – комплекс криминогенно значимых социальных, политических, экономических и правовых отношений, складывающихся в информационной сфере и детерминирующих состояние преступности в сфере компьютерной информации.

Предмет исследования – практика функционирования информационной сферы; уголовно-правовые отношения, возникающие в результате преступного использования компьютерных технологий; меры криминологического, уголовно-правового и организационного характера, способные, в конечном счете, обеспечить безопасность информационных отношений.

Цель и основные задачи исследования. *Цель исследования* – теоретико-прикладное изучение феномена компьютерной преступности; формулирование положений, составляющих теоретические основы

криминологического и уголовно-правового анализа компьютерной преступности; выработка на этой основе предложений по совершенствованию правовых и организационных основ противодействия ей; развитие теории отечественного уголовного права и криминологии в этой сфере.

В соответствии с целью были поставлены следующие основные з*адачи исследования*:

- провести статистический и криминологический анализ современного состояния компьютерной преступности, охарактеризовать основные тенденции её развития;

- раскрыть социальную и правовую сущность компьютерной преступности, сформулировать теоретическую модель системы компьютерных преступлений, составляющих содержание компьютерной преступности, а также современное понятие «компьютерная преступность»;

- осуществить криминологическую характеристику личности компьютерного преступника и выделить основные типы;

- провести комплексный анализ феномена компьютеризации общества, обосновать тезис о социальной значимости компьютеризации, определить характер её криминогенного влияния на возникновение компьютерной преступности;

- исследовать и охарактеризовать основные причины и иные криминогенно значимые факторы детерминации компьютерной преступности в современных условиях России;

- рассмотреть проблему компьютерной игромании и её влияния на компьютерную преступность;

- проанализировать спектр виктимологических проблем компьютерной преступности;

- обосновать предложения по совершенствованию уголовного законодательства и рекомендации для следственной и судебной практики

по квалификации общественно опасных деяний в сфере компьютерной информации на основе общего юридического анализа признаков, характеризующих элементы составов данных преступлений;

- рассмотреть проблему противодействия компьютерной преступности на концептуальном, законодательном и организационном уровнях;

- провести сравнительное исследование отечественного и международного опыта решения правовых, организационных и иных проблем предупреждения компьютерных преступлений.

Методология и методы исследования. Методологическую основу исследования составляет системный анализ криминологических аспектов государственных, общесоциальных, экономических, технических и правовых предпосылок текущего состояния компьютерной преступности в Российской Федерации. В ходе работы использованы такие общенаучные методы, как анализ и синтез, дедукция и индукция, исторический и логический методы, восхождение от абстрактного к конкретному, посредством которых осуществлялась теоретическая интерпретация научного и эмпирического материала для формирования выводов и предложений.

В процессе исследования использовались частнонаучные методы: системно-структурный, формально-юридический, сравнительно-правовой, статистические, системного анализа, сравнительного правоведения, конкретно-социологического исследования, контент-анализ.

Применение вышеизложенных научных методов, сохранение приоритета за соблюдением принципа взаимосвязи общего, особенного и единичного, исторического и логического, абстрактного и конкретного, обеспечило выполнение требований комплексного и междисциплинарного подходов к диссертационному исследованию.

Теоретической базой исследования послужили работы ведущих отечественных и зарубежных ученых в области теории информации,

криминологии, уголовного, конституционного, административного и гражданского права, а также по некоторым другим отраслям права, философии, социологии, психологии, относящиеся к исследуемой проблеме. В процессе работы над диссертацией были изучены основные государственные концепции и теоретические подходы отечественных и зарубежных ученых к проблемам компьютерной преступности, информационной безопасности и противодействию преступности в сфере компьютерной информации, информационные материалы полиции зарубежных стран и Интерпола, публикации в сети Internet, посвященные проблемам противодействия компьютерным преступлениям, в том числе официальные материалы правоохранительных органов зарубежных стран и Российской Федерации.

Нормативно-правовую базу диссертации составили: Конституция Российской Федерации, УК РФ 1996 г., действующее отраслевое законодательство, законы и подзаконные нормативные акты, международное законодательство по проблемам компьютерной преступности, федеральные программы по укреплению правопорядка и профилактике преступности.

Эмпирическую базу составили статистические данные, отражающие криминологическую обстановку как в целом по стране, так и в разрезе преступлений в сфере компьютерной информации с 1997 по 2005 г.г. Исследована и обобщена вся опубликованная судебная практика по рассмотренным за период с 1997 по 2005 г. уголовным делам о преступлениях в сфере компьютерной информации: приговоры, определения и постановления судов различных инстанций. Изучено уголовное законодательство стран Европы, США, Канады, государств-участников Содружества Независимых Государств по проблемам компьютерной преступности; рекомендации международных организаций по проблемам уголовно-правового регулирования общественных отношений в информационной сфере.

По предварительно составленной рабочей программе изучено 110 уголовных дел, возбужденных за совершение преступлений в сфере компьютерной информации. В рамках проведенного автором конкретно-социологического исследования собрана, изучена и обобщена практика деятельности 138 органов государственной власти и управления, предприятий, организаций, и учреждений в сфере обеспечения информационной безопасности. Проведено анкетирование более 200 работников правоохранительных органов (в том числе суда и прокуратуры) по вопросам правоприменительной деятельности в сфере компьютерной информации. В интервьюировании и анкетировании приняли участие 274 молодых людей в возрасте 19–22 лет, 150 подростков–постоянных членов компьютерных клубов на предмет подверженности компьютерной зависимости. Использованы опубликованные данные иных социологических и криминологических исследований, касающиеся проблем компьютерной преступности.

Научная новизна исследования. Данное исследование является одним из первых на диссертационном уровне, где проблемы компьютерной преступности рассмотрены не только с теоретико-правовых позиций, позиций уголовно-правовой защиты, но и под углом зрения криминологической науки. Диссертация является комплексным, логически цельным и завершенным монографическим исследованием, посвященным обоснованию теоретико-концептуального видения проблем компьютерной преступности и её предупреждения с использованием научного аппарата социологии, психологии, конституционного, уголовного, международного и некоторых других отраслей права. В отличие от других работ, рассмотрен психологический компонент компьютерных преступлений, в особенности игровые мотивации совершения преступлений.

Новизна работы заключается также и в том, что проведенное автором исследование позволило вскрыть и проанализировать многие особенности компьютерной преступности, которые ранее не получали доктринальной

оценки. Направленность и содержательное решение поставленных задач позволяет считать данное исследование определенным научным вкладом в развитие отечественной криминологии, информационных правоотношений, которое должно дополнить отдельные разделы юридической науки и способствовать созданию методологических основ формирования нового научного направления – компьютерной криминологии.

Основные исследовательские подходы и сформулированные в диссертации положения, указывающие на её научную новизну, сводятся к следующему:

- осуществлена развернутая криминологическая характеристика и определены основные тенденции современного состояния компьютерной преступности с учетом трансформации современного российского общества в общество информационное;

- раскрыты понятие и сущность феномена «компьютерная преступность», сформулирована авторская дефиниция понятия компьютерной преступности;

- установлены элементы социального генезиса в процессе компьютеризации как позитивного социально значимого явления, которое опосредует негативно-криминальные и также социально значимые проявления в сфере компьютерной информации;

- реализован авторский подход к изучению компьютерной игромании как разновидности девиантного поведения и одной из причин компьютерной преступности;

- дана характеристика виктимологического аспекта компьютерной преступности как особого среза общественных отношений, реализуемых в процессе информационного обмена;

- выделены виктимологические факторы компьютерной преступности, которые рассмотрены как единый причинно связанный процесс, находящийся в определенной опосредованной связи с

компьютерными преступлениями;

- дана теоретико-прикладная разработка критериев классификации и типологии личности компьютерного преступника;

- раскрыто содержание противодействия компьютерной преступности как особого вида деятельности в области социального управления, осуществляемого в рамках социально-правовой функции государства;

- предложена система мер противодействия компьютерной преступности, а также сформулирован общий алгоритм создания системы безопасности самостоятельного объекта информационного обмена;

- выдвинуты, сформулированы и обоснованы предложения по совершенствованию действующего законодательства, регламентирующего ответственность за преступления в сфере компьютерной информации;

- показаны конкретные направления международного сотрудничества в области противодействия компьютерной преступности;

- аккумулирован и обобщен теоретический опыт, накопленный учеными в области уголовного права, криминологи других отраслей права и нашедший отражение в научных трудах, посвященных проблемам компьютерной преступности, аргументированы собственные конструктивные суждения об оптимально приемлемом решении соответствующих вопросов.

Теоретическая и практическая значимость исследования. Настоящее диссертационное исследование направлено на решение крупной социально-правовой проблемы на современном этапе развития нашего государства и представляет собой определенную теоретическую основу для последующих научных исследований по данной теме.

Теоретические положения, выводы и рекомендации, в частности, криминологическая характеристика компьютерной преступности, феноменология и тенденции её развития, особенности личности компьютерного преступника, причинного комплекса, её уголовно-правовая

характеристика, а также критический анализ теоретического опыта, отраженного в научных трудах, посвященных исследуемой проблеме, могут быть использованы:

– при проведении дальнейших научных исследований проблемы противодействия компьютерной преступности на федеральном и региональном уровнях;

– в учебном процессе по курсам «Криминология», «Уголовное право», преподаваемых на юридических факультетах высших учебных заведений России;

– при подготовке учебников, учебных и практических пособий, комментариев, лекций, методических рекомендаций по уголовному праву и криминологии, посвященных темам и вопросам, касающимся компьютерной преступности.

Избранный путь решения проблем компьютерной преступности позволяет выработать новые научно обоснованные рекомендации по обеспечению криминологической безопасности информационной сферы.

Практическая значимость диссертационного исследования определяется комплексом предложений по совершенствованию уголовно-правовых, специально-криминологических и организационных основ противодействия компьютерной преступности. Положения, обобщения, выводы, рекомендации и предложения, представленные в исследовании, могут способствовать решению проблемы обеспечения информационной безопасности самостоятельных объектов информационного обмена.

Выводы и практические предложения дают возможность совершенствования законотворчества с учетом изменений информационных отношений, требующих уголовно-правовой охраны, могут быть использованы при корректировке криминологической политики России в данной сфере, при разработке постановления Пленума Верховного суда Российской Федерации по проблемам компьютерной преступности.

В диссертации созданы информационные и методические предпосылки для повышения эффективности профессиональной подготовки специалистов в области расследования (в том числе раскрытия) преступлений в сфере компьютерной информации; при квалификации криминальных проявлений в информационной сфере и отграничении от смежных составов преступлений; в практической деятельности сотрудников правоохранительных структур при планировании и разработке профилактических мероприятий, направленных на предупреждение совершения компьютерных преступлений.

Полученные результаты могут быть использованы в других теоретических и прикладных целях.

Основные положения, выносимые на защиту. На защиту вынесены следующие наиболее значимые и существенные положения из характеризующих научную новизну диссертационного исследования:

1. Под компьютерной преступностью следует понимать совокупность совершенных на определенной территории за определенный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности.

2. Характеристика информатизации общества в единстве трех составляющих: медиатизации, интеллектуализации, компьютеризации и рассмотрение последней как технократического, гуманитарного, государственно-правового процесса, процесса социального риска и криминологического процесса, посредующего возникновение преступлений, совершаемых с использованием компьютерной техники и информационных технологий.

3. Выделяются следующие основные тенденции развития компьютерной преступности в России: а) высочайшие темпы роста; б)

корыстная мотивация большинства совершенных компьютерных преступлений; в) усложнение способов совершения компьютерных преступлений и появление новых видов противоправной деятельности в сфере компьютерной информации; г) рост криминального профессионализма компьютерных преступников; д) омолаживание компьютерных преступников и увеличение доли лиц, ранее не привлекавшихся к уголовной ответственности; е) рост материального ущерба от компьютерных преступлений в общей доле ущерба от прочих видов преступлений; ж) перенос центра тяжести на совершение компьютерных преступлений с использованием компьютерных сетей; з) перерастание компьютерной преступности в разряд транснациональной преступности; и) высокий уровень латентности компьютерных преступлений.

4. Классификация латентных групп в сфере компьютерной информации: а) противоправные деяния, совершенные по небрежности в силу неосведомленности самого пользователя-правонарушителя об их преступном характере; б) противоправные деяния, о которых потерпевшая сторона не сообщает в правоохранительные органы в силу собственной незаинтересованности; в) противоправные деяния, где нет явно выраженной потерпевшей стороны; г) противоправные деяния, которые известны узкому кругу лиц; д) неучтенные правоохранительными органами преступления в сфере компьютерной информации; е) нераскрытые (неполно раскрытые) преступления в сфере компьютерной информации.

5. Определение круга преступлений, могущих быть включенными в криминологическое содержание понятия компьютерной преступности: а) преступления, затрагивающие сферу компьютерной информации; б) общеуголовные преступления, совершенные с использованием возможностей компьютерных технологий; в) сетевые компьютерные преступления; г) трансграничные киберпреступления.

6. Предложена авторская типологизация компьютерных преступников на профессиональный, криминогенный тип и психотип на основе характеристик выделенных классифицированных групп (в зависимости от формирования негативной направленности личности; мотивации; уровня профессиональной подготовки; социального положения; противоправной направленности; возможности доступа к средствам компьютерной техники; по организационному признаку).

7. Авторская криминологическая концепция игромании, включающая:

– рассмотрение игры как социально значимого, личностного явления, носящего исторический характер и призванного закреплять жизненные позиции личности;

– рассмотрение компьютерной игры как криминологического фактора, обусловленного проникновением компьютерных технологий в сферу частной жизни, существенным изменением природы межличностного общения и появлением нового вида общения – виртуального, задающего негативные нравственно-психологические качества личности, которые проявляются в мотивации преступного поведения;

– действие «эффекта ореола» компьютерной игры, выражающегося в способности обучения насильственным агрессивным действиям посредством усвоения правил поведения, соблюдаемых и демонстрируемых «героями» компьютерных игр;

– определение игрового влечения как приобретенного стойкого желания виртуального уединения, способа самореализации и удовлетворения глубинных личностных желаний;

– классификация мотивации компьютерных игр: а) ради испытания собственных интеллектуальных способностей; б) из азартно-корыстных соображений; в) ради игрового удовольствия или из скуки и формулирование соответствующих типов игроков;

– выделение в структуре игрового мотива преступного поведения в сфере компьютерной информации двух уровней: а) осознанного или предметного, выполняющего функцию непосредственного удовлетворения явных, лежащих на поверхности игровых потребностей, б) бессознательного, в рамках которого игрок, даже не желая этого, приобретает стереотипные поведенческие навыки и эмоциональные реакции.

8. Определение жертв компьютерных преступлений как субъектов информационного обмена, с одной стороны, непосредственно пострадавших от преступления, независимо от того, признаны формально потерпевшими или нет, с другой в той или иной мере являющиеся носителями реализованной виктимности, и классификация их на физических лиц и социальные общности людей в разной степени интеграции.

9. Характеристика факторов криминогенно-виктимогенной детерминации, провоцирующих возможность совершения компьютерных преступлений, и подразделение их на индивидуально-личностные (социально-психологические), социальные (положение потенциальной жертвы преступления в социальной иерархии общества), поведенческие (деятельностные), а также выделение фактора технической уязвимости компьютерных технологий.

10. Предлагается многофакторная модель совершенствования противодействия компьютерной преступности, включающая:

– рассмотрение противодействия как особого вида деятельности в области социального управления, призванного в рамках социально-правовой функции государства планомерно влиять на общество путем поддержания в нем нормативного порядка (средствами позитивного и репрессивного правового контроля) и минимизации девиантного поведения;

– двойственный подход к содержательному наполнению мер противодействия компьютерной преступности, которые, с одной стороны, направлены на сокращение преступлений в сфере компьютерной информации, известных уголовному праву. С другой – на нейтрализацию негативных криминогенных процессов в информационной сфере. На общесоциальном уровне – это решение социально-экономических и иных проблем функционирования информационной сферы; на специальном – воздействие на информационную микросреду, виды и формы преступного поведения в сфере компьютерной информации; на индивидуальном – позитивное изменение системы ценностей пользователей ЭВМ, систем ЭВМ или их сети, внедрение морально-этических правил при использовании возможностей информационных технологий;

– формулирование системы мер противодействия компьютерной преступности с позиции комплексного подхода, при котором охватывается все многообразие факторов (правовых, экономических, политических, психологических, воспитательных), оказывающих влияние на формирование криминогенных свойств личности. При этом меры, ориентированные на социальную и личностную сферы бытия пользователей ЭВМ, систем ЭВМ или их сети, выходят за пределы функционирования системы правоохранительных органов, и объединяют организационно-управленческий, кадровый и технический уровни;

– разработка общего алгоритма безопасности ЭВМ, системы ЭВМ или их сети в рамках интегрированной системы, объединяющей многообразие средств защиты на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных.

11. Предложения по совершенствованию законодательства, регламентирующего ответственность за компьютерные преступления по Уголовному кодексу РФ, на основе уточнения признаков отдельных составов преступлений в сфере компьютерной информации и круга их субъектов:

а) уточнить редакцию ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ» введением в диспозицию части 1 указания на цель как обязательный признак субъективной стороны состава преступления; часть 2 указанием на признак «совершение группой лиц по предварительному сговору или организованной группой»; часть 2 ст. 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» указанием на признак «причинение существенного вреда»;

б) дополнить статью 242.1 УК РФ «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних» частью третьей следующего содержания: «Производство детской порнографической продукции с целью распространения через ЭВМ, систему ЭВМ или их сеть, предложение или предоставление в пользование, распространение либо приобретение детской порнографии через компьютерную систему для себя или для другого лица, - наказывается лишением свободы на срок от десяти до двенадцати лет»;

в) дополнить ст. 20 УК РФ «Возраст, с которого наступает уголовная ответственность» указанием на ст. 273 УК «Создание, использование и распространение вредоносных программ для ЭВМ»;

г) дополнить гл. 28 раздела IX УК РФ самостоятельными составами, предусматривающими уголовную ответственность за мошенничество с использованием компьютерных технологий и подлог с использованием компьютерных технологий.

12. Стратегия международного сотрудничества в сфере противодействия компьютерной преступности и приоритетные направления ее реализации, в том числе: межгосударственные соглашения, организация межгосударственной оперативно-розыскной деятельности, принятие межгосударственного регламента и совершенствование интеграционных процессов в рамках межгосударственных организаций,

обоснование необходимости разработки и принятия соответствующей комплексной межгосударственной программы.

Достоверность и обоснованность результатов исследования обеспечивались использованием многократно апробированных в науке уголовного права и криминологии специальных научных методов, взаимным сопоставлением данных, полученных различными методами и из разных источников, соблюдением требований репрезентативности и валидности отобранного для изучения материала, обобщением практического опыта. Указанная информация и данные эмпирического исследования применялись для аргументирования теоретических выводов, предложений и рекомендаций, нашедших отражение в диссертации.

Апробация и внедрение результатов диссертационного исследования

Основные положения, выводы, рекомендации и предложения, содержащиеся в настоящем диссертационном исследовании, отражены:

– в деятельности Аппарата Совета Федерации Федерального Собрания Российской Федерации в части совершенствования информационного обеспечения законодательного процесса в области противодействия преступности в сфере высоких технологий;

– правоприменительной практической деятельности органов предварительного следствия в системе МВД России при расследовании уголовных дел по преступлениям в сфере компьютерной информации;

– аналитических материалах по противодействию криминальным проявлениям в информационной сфере, используемых администрацией Смоленской области при разработке Комплексной региональной программе по борьбе с преступностью на 2007-2010 г.г.;

– научной деятельности Академии управления МВД России; Института гуманитарного образования (г. Москва), Московского университета МВД России (Смоленский филиал), Смоленского гуманитарного университета;

– учебном процессе ряда высших учебных заведений, в том числе в разработанной учебной программе специального курса «Проблемы компьютерной преступности»;

– отражены в 42 опубликованных автором научных работах, в том числе в двух монографиях и шести учебных пособиях;

– в выступлениях автора на семи международных, трех республиканских и иных научно-практических конференциях. В частности: на международных конференциях «Теория, история, практика и методология современной юриспруденции (Петропавловск, 2002 г.); «Университеты и региональное развитие (Смоленск, 2002 г.); «Десять лет Конституции России в зеркале юридической науки и практики» (Москва, 2003 г.); «Информатизация и информационная безопасность правоохранительных органов» (Москва, 2005) и др.; на Всероссийских научно-практических конференциях «Правовые проблемы экономической, административной и судебной реформы в России» (Москва, 2004 г.); «Профилактика безнадзорности и правонарушений несовершеннолетних» (Смоленск, 2004 г.); «Третьи Авраамиевские чтения» (Смоленск, 2005 г.).

Структура диссертации. Диссертация состоит из введения, четырех глав, объединяющих 17 параграфов, заключения, списка использованной литературы и приложений, включающих образцы применявшегося в ходе диссертационного исследования социологического инструментария.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации; определяются объект, предмет, цели и задачи работы; характеризуются её методологические, теоретические основы, эмпирическая база; раскрываются научная новизна, а также теоретическое и практическое значение; сформулированы основные положения, выносимые на защиту; излагаются сведения об апробации полученных результатов и внедрении их в практику.

В первой главе «Теоретико-криминологическая характеристика компьютерной преступности», состоящей из четырех параграфов, формулируется понятие «компьютерная преступность», раскрывается её социальная и правовая сущность, характеризуются основные тенденции, рассматривается проблема её латентности и типологии.

Первый параграф первой главы *«Понятие компьютерной преступности»* посвящен обоснованию теоретического определения «компьютерная преступность». Анализируя существующие научные подходы, автор отмечает их непреходящее значение для становления концептуальных представлений в рассматриваемой сфере, поскольку система взглядов на данный вопрос достаточно разнообразна и противоречива.

В работе представлена развернутая характеристика существующих дефиниций отечественных и зарубежных ученых понятия «компьютерное преступление» как необходимой предпосылки к пониманию общего понятия «компьютерная преступность», в основе которого лежит статистическая совокупность последних. Понятие «компьютерное преступление» рассматривается с уголовно-правовых, криминалистических и криминологических позиций и определяется как общественно опасное деяние с использованием компьютера в целях

извлечения выгоды, которое нанесло или могло нанести ущерб, а также иное незаконное использование компьютера в совершении преступления.

Формулируется вывод о неидентичности понятий «компьютерная преступность» и "преступность в сфере компьютерной информации". Излагается два подхода к пониманию компьютерной преступности, в соответствии с которыми компьютерная преступность в «узком значении» включает все преступления в сфере компьютерной информации, а также преступления с использованием компьютерных технологий, в «широком значении» связана с информационной преступностью, являясь его сердцевиной, важной составной частью.

В итоге диссертант приходит к выводу, что компьютерная преступность представляет собой совокупность совершенных на определенной территории за определенный период преступлений (лиц, их совершивших), непосредственно посягающих на отношения по сбору, обработке, накоплению, хранению, поиску и распространению компьютерной информации, а также преступлений с использованием компьютера в целях извлечения материальной выгоды или иной личной заинтересованности.

Второй параграф первой главы *«Компьютерная преступность как объект исследования в отечественной и зарубежной криминологии»* посвящен содержательной характеристике компьютерной преступности как общественно опасного массового социального явления, базирующегося на уголовно-правовом понятии преступления, и определению его границ.

Автор обращается к рассмотрению законодательного опыта в формулировании института компьютерных преступлений стран СНГ и Балтии и подразделяет их на три группы: 1) преступления, в которых объектом преступного посягательства выступает компьютерная информация; 2) преступления, в которых компьютерная информация является орудием или средством совершения другого преступления; 3) преступления, совершаемые с использованием компьютерной техники в

той или иной мере. Анализируются терминологические расхождения, имеющие место в содержательном понимании компьютерной преступности в европейских странах и у отечественных ученых.

Делается вывод о том, что, имея безусловную связь с электронной формой обработки информации посредством компьютерной техники, компьютер может выступать в разных ипостасях: а) быть инструментом преступной деятельности; б) хранилищем компьютерной информации (с одновременным выполнением функций по её обработке); в) использоваться как средство подготовки преступного посягательства; г) выступать предметом преступного посягательства.

Своим содержанием компьютерная преступность охватывает разнообразные виды причинения вреда охраняемым законом интересам личности, общества и государства в разных сферах: в сфере экономики, безопасности, военной сфере, конституционной, сфере нравственности, общечеловеческих ценностей, уголовно-правовой.

Рассматривая компьютерную преступность как некий феномен, оказывающий непосредственное влияние на современную преступность в целом, и как её подструктуру в частности, выделяются группы преступлений, составляющих структуру и формирующих содержание компьютерной преступности: а) преступления, в которых охраняемая законом компьютерная информация является основным объектом посягательства; б) общеуголовные преступления, совершенные с использованием возможностей компьютерных технологий; в) сетевые компьютерные преступления, совершаемые с использованием компьютерных технологий в виртуальной среде – пространстве, в котором осуществляются сетевые процессы, существенно отличающиеся от простого обмена данными между компьютерами; г) трансграничные киберпреступления, затрагивающие интересы граждан или юридических лиц других стран, совершаемые в рамках «всемирной паутины» –

пространстве, в котором отсутствуют географические и геополитические границы государств и не действует их юрисдикция.

Третий параграф первой главы *«Основные тенденции компьютерной преступности в России и проблемы её латентности»* посвящен анализу состояния компьютерной преступности, содержащему структурные, динамические и иные криминологически значимые характеристики и особенности, основанному на статистических данных за период с 1997 по 2005 г.г.

Как свидетельствует уголовная статистика, научно-криминологические и иные информационно-аналитические данные, указанный период характеризуется устойчивым ростом исследуемого вида преступности: с 33 – в 1997 г. до 10214 – в 2005 г. В то же время число выявленных лиц, их совершивших, возрастало гораздо медленнее и только к 2004 году превысило 1030 человек. Анализируя динамику, автор констатирует, что за последние два года рост неправомерного доступа к охраняемой законом компьютерной информации (ст. 272 УК РФ) составил 113%, создания, использования и распространения вредоносных программ для ЭВМ (ст. 273 УК РФ) – 146%. Нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ) с 2002 года имеют тенденцию уменьшения количества регистрируемых преступлений и выявленных лиц, их совершивших.

Качественная характеристика свидетельствует о том, что свыше 80% умышленных преступлений в сфере компьютерной информации носят корыстный характер. Преобладающими выступают деяния, связанные с распространением вредоносных программ (18,6%), реже – получение безвозмездного программного продукта с последующей его продажей (5,7%) и внесение изменений в различные электронные реестры имущества (2,9%).

Высокие темпы роста компьютерных преступлений характеризуются совершенствованием технологий совершения преступлений, осваиванием

новых видов противоправной деятельности в сфере компьютерной информации: роумерское мошенничество, использование сотовых телефонов-двойников, неправомерный доступ к телекоммуникационным ресурсам цифровых мини-АТС, имеющих выход в общегосударственную телефонную сеть, к каналам коммерческого спутникового телевидения и другие, – т. е. ростом профессионализма компьютерных преступников. Из 1673 уголовных дел, возбужденных по материалам региональных подразделений управления «К» МВД России в первом полугодии 2005 г., 55% связаны с неправомерным использованием сетевых реквизитов при авторизации в сети Интернет; 10,6% проходят как "компьютерное пиратство"; 8% связаны с распространением порнографии; 4,1% возбуждены по фактам распространения вредоносных программ.

Подавляющая часть компьютерных преступлений носит экономическую направленность и связана с нанесением значительных финансовых убытков. Обработка данных об имеющемся в России компьютерном парке позволяет прогнозировать рост компьютерных преступлений в 2006 году до 12000. Если учесть, что средний ущерб от одного компьютерного преступления составляет порядка 10 тыс. долларов США, то можно с определенной степенью достоверности прогнозировать ущерб от компьютерных преступлений в России порядка 100-150 млн. долларов.

Среди тенденций компьютерной преступности выделяется увеличение доли лиц, ранее не попадавших в сферу внимания правоохранительных органов, технически грамотных, оснащенных современнейшей компьютерной техникой. Если в 1997–1999 годах преступления в сфере компьютерной информации в основном совершались лицами старшего возраста, то, начиная с 2000 года, прослеживается тенденция омоложения компьютерных преступников.

Автор уделяет внимание исследованию тенденции роста латентности компьютерной преступности и выделяет имеющую место в обществе

парадоксальную ситуацию, когда, с одной стороны, совершенные компьютерные преступления не попадают в поле зрения правоохранительных органов, а с другой – факты противоправной деятельности в сфере охраняемой законом компьютерной информации не находят должного осуждения у потерпевшей стороны. Автор констатирует, что причины высокого уровня латентности компьютерной преступности лежат как в области объективных, так и субъективных факторов, которые обстоятельно проанализированы в работе.

Логика исследования предопределила необходимость анализа признаков латентности компьютерных преступлений и выделение на их основе латентных групп в виде противоправных деяний в сфере компьютерной информации: а) совершенных по небрежности; б) не сообщенных потерпевшей стороной в правоохранительные органы; в) с неустановленными виновными лицами; г) известных узкому кругу лиц; д) неучтенных правоохранительными органами; д) нераскрытых или неполно раскрытых следственными органами.

Четвертый параграф первой главы *«Типология компьютерной преступности»* посвящен обобщению и систематизации типичных черт компьютерных преступлений, а также свойств и качеств личности компьютерного преступника как необходимой основы методики прогнозирования криминального поведения в информационной сфере и применения дифференцированных и индивидуализированных предупредительных мер.

Анализируя преступную компьютерную деятельность, автор рассматривает её как результат криминального проявления профессиональной деятельности (или деятельности, содержащей элементы профессионализма), связанной со знанием компьютерных технологий, которая может осуществляться под прикрытием законной экономической деятельности или непосредственно в процессе иной служебной деятельности. Компьютерные преступления, обладая определенной

технической специфичностью, также характеризуются и тем, что информационная сфера может являться как основным объектом посягательства, так и непосредственным факультативным. Компьютерная преступность рассматривается не только как социальное явление, предопределенное развитием общественных отношений рыночного характера, выраженное в криминальной форме и направленное против интересов личности, общества и государства в информационной сфере, но и как сложное специфическое системно-структурное образование с особыми аддитивными свойствами.

Учитывая, что типичность преступлений обусловливается определенным шаблонным характером способов их осуществления, многократностью повторения мотивации преступной деятельности, автор выделяет группы компьютерных преступлений*:* а) экономические преступления, б) преступления против личных прав (в том числе неприкосновенности частной сферы), в) преступления против общественной безопасности и общественного порядка.

Исходя из сложившихся в теории криминологии подходов, с опорой на отечественные криминологические источники и собственные проведенные исследования, в работе осуществлена классификация компьютерных преступников в зависимости от формирования негативной направленности личности; уровня специального образования; мотивации; уровня профессиональной подготовки; социального положения; характера противоправной направленности; возможности доступа к средствам компьютерной техники и по организационному признаку.

Указанные группировки позволили диссертанту определенным образом систематизировать контингент преступников, основываясь на выделении существенных признаков, причинно связанных с преступным поведением. В основу типологии были положены признаки-причины, обеспечивающие содержательные характеристики и определенные динамические закономерности, детерминирующие линии поведения. В

частности выделены следующие типы компьютерных преступников: а) профессиональный тип (лица с ярко выраженными корыстными целями и индивидуально-эгоистической мотивацией), б) криминогенный тип (лица, сочетающие знания компьютерной техники, навыки программирования, с элементами фанатизма), в) психотип (лица, страдающие компьютерными фобиями, а также неболезненными формами интернет-зависимости или компьютерной игроманией). Знание характерных черт выделенных типов компьютерных преступников, по мнению автора, необходимы при планировании и реализации предупредительных мер, направленных на снижение криминогенной активности соответствующих субъектов.

Во второй главе «Причинный комплекс компьютерной преступности», состоящей из пяти параграфов, рассмотрены криминогенные факторы, обусловливающие существование и рост компьютерной преступности, в том числе виктимологические аспекты.

Первый параграф второй главы «Компьютеризация как предпосылка возникновения компьютерной преступности» посвящен анализу происходящей в обществе информационной революции, которая является следствием двух параллельно развивающихся процессов: возрастания роли и увеличения объемов информации и совершенствования компьютерных технологий накопления и распространения информации.

Процесс информатизации общества рассмотрен в единстве трех составляющих: *медиатизации* – процесса совершенствования средств сбора, хранения и распространения информации; *интеллектуализации* – процесса развития способности восприятия и порождения информации; *компьютеризации* – процесса совершенствования средств поиска и обработки информации. В рамках исследования автор подробно останавливается на компьютеризации как социально значимом явлении и многоуровневом процессе: технократическом, повышающем информационный уровень развития общества; гуманитарном, кардинально меняющем уровень социальной сферы общества и трансформирующем

человека в «био-социально-техногенное» явление; государственно-правовом, оказывающем влияние на состояние и структуру государственного управления и правового регулирования; социального риска, обладающем возможностью нарушения состояния общественной безопасности; криминологическом, посредующем возникновение преступлений с использованием компьютерной техники и информационных технологий. Противоправное использование последних на основе существующих в обществе противоречий и с учетом индивидуально-личностных особенностей компьютерных преступников выделены в качестве факторов, стимулирующих возникновение и прогрессирующее существование компьютерной преступности.

Второй параграф второй главы «Общесоциальные причины компьютерной преступности» посвящен исследованию причинного комплекса компьютерной преступности в условиях формирования и становления в Российской Федерации информационных отношений.

По мнению диссертанта, компьютерная преступность, являясь составной частью общей преступности, порождается общими причинами, которые включены в систему социальных противоречий общества и обусловлены сложным взаимодействием объективных условий и субъективных внутренних факторов, то есть среды и личности. Такой подход позволил рассмотреть ряд ключевых теоретических вопросов, дать анализ конкретных процессов, порождающих компьютерную преступность, рассмотреть группы экономических, общесоциальных причин и причин правового характера.

Исходя из результатов анализа причинного комплекса, определяющего тенденцию роста компьютерной преступности, автор утверждает, что противоправное поведение, посягающее на охраняемую законом компьютерную информацию, выступает конкретным результатом не только социальных противоречий, но и противоречий в информационной сфере, которая существует внутри общества, пронизывая

все области его жизнедеятельности, расширяя рамки социальной среды человека и преломляя обшесоциальный причинно-следственный комплекс противоречий.

Автор приходит к выводу, что социальная сущность криминогенных причин и условий совершения компьютерных преступлений определяется во взаимосвязи с основными закономерностями развития общества и существующими в нем противоречиями. При этом связь между компьютерной преступностью и её детерминантами двухсторонняя. С одной стороны, эти детерминанты порождают компьютерную преступность во все расширяющихся масштабах. С другой стороны, масштабная криминализация информационной сферы обостряет негативную ситуацию в ней и препятствует цивилизованному развитию в России информационного сектора.

Третий параграф второй главы «Личность компьютерного преступника и индивидуально-личностные причины компьютерной преступности» посвящен вопросам взаимодействия человека с социальной средой и анализу возникающих при этом противоречий, решение которых предопределяет выбор его поведения.

Природа этих противоречий различна. Одна группа противоречий имеет психологическую природу. Другая – это противоречия между психологией личности и реальностью. Третья группа имеет объективную социальную природу, предопределяя возникновение двух предыдущих групп. Автор, анализируя каждую группу противоречий, обращает внимание на то, что наличие у компьютерных пользователей личностных социально-психологических особенностей или деформаций обусловливает совершение ими конкретного уголовно-противоправного деяния и выступает индивидуально-личностной причиной компьютерного преступления.

Экономические и социальные отношения, влияя на преступность, не предопределяют ее в конкретных случаях, поскольку все, что происходит в

жизни, проходит через сознание человека, а оно, хотя и зависит от общих закономерностей, но не является их игрушкой. Сделан вывод о том, что в основе существования компьютерной преступности лежит противоправное использование возможностей компьютерных технологий на базе существующих в обществе противоречий, но с учетом индивидуально-личностных особенностей компьютерных преступников.

Вместе с тем диссертантом констатируется, что в обществе с развитыми информационными отношениями развиваются ранее неизвестные формы взаимодействия и общения территориально удаленных компьютерных пользователей, формируются новые формы социальных взаимосвязей, социальных отклонений и психических расстройств. В связи с охватившим современное общество процессом всеобщей компьютеризации имеет место «виртуализация» духовной жизни, которая отделяет компьютерных пользователей от человеческого социума. Это может привести к патологическим изменениям психики – компьютерным фобиям, когда человек становится «вещью в себе» в результате болезненного деформирования психики, вызванного постоянным использованием информационных технологий. Как следствие, социальная изоляция – состояние, связанное с усилением в человеке психологии индивидуализма, с абстрагированием от окружающей социальной среды обитания и общения.

В отдельную группу диссертантом выделены лица, страдающие непатологическими формами компьютерной зависимости с пограничным расстройством психики. Нездоровое пристрастие к многочасовому времяпрепровождению за компьютером, систематическое пребывание в Inernet может привести к непатологическим формам зависимости («интернет-зависимость», игромания), к социальной дезадаптации, нарушению имеющихся общественных связей. В подобной зависимости автор усматривает определенную параллель между компьютерным пристрастием и влечением других людей к алкоголю или наркотикам.

Виртуальный вид общения задает новые качества личности, а компьютерная зависимость из личностного фактора трансформируется в криминологический.

Результаты проведенного исследования, характеристики социально-личностных и социально-психологических особенностей компьютерных преступников, обусловливающих совершение уголовно-противоправных деяний в сфере компьютерной информации, позволили сформулировать основные индивидуально-личностные причины совершения компьютерных преступлений, среди которых выделены группы объективного и субъективного уровней.

Четвертый параграф второй главы «Компьютерная игромания как разновидность девиантного поведения и одна из причин компьютерной преступности» посвящен проблеме игромании – механизму криминогенного воздействия информации, распространяемой с помощью ЭВМ, системы ЭВМ или их сети, посредством привыкания к компьютерным играм.

Автор обращает внимание на особую опасность, которую представляет эпидемия игромании. Исследование, проведенное среди подростков, регулярно посещающих специализированные компьютерные клубы, позволило выявить у них в основной массе наличие навязчивого желания играть в компьютерные игры. С этой целью посещают клуб ежедневно – 4%; 3-4 раза в неделю – 10%; 1-2 раза в неделю – 50%; периодически – 36%.

Но игра, как утверждают психологи, – это не простое времяпрепровождение, это более сложные отношения и социальные связи. Игра в социальном понимании выполняет важную функцию, она закрепляет жизненные позиции личности и помогает в выборе своей роли в обществе. Распространение компьютерных технологий способствует изменению эталонов социализированности человека, формированию образцов поведения и стереотипных форм активности пользователей,

которые трансформируются в своеобразную виртуальную субкультуру, виртуальный мир, в котором жизнь – это игра. Это воздействие вызывает в личности такие глубинные трансформации, что человек освобождается от социальных запретов.

Автор рассматривает компьютерную игровую зависимость не только как социально значимое и личностное явление, но и как криминологический фактор. В работе рассмотрено действие «эффекта ореола» компьютерной игры, выражающееся в способности обучению насильственным агрессивным действиям посредством усвоения правил поведения, демонстрируемых «героями» компьютерных игр. Компьютерные игры рассмотрены в более сложных формах проявления, когда пользователь, с одной стороны, удовлетворяет потребность в игре, в острых эмоционально возбуждающих ощущениях. С другой стороны, способы удовлетворения игрового азарта для него перестают иметь решающее значение. Компьютер используется для совершения преступления, которое воспринимается как своеобразная азартная (но уже носящая криминальный характер) игра.

Изучение поведения пользователей позволило сделать вывод о разной мотивации компьютерной игры: а) ради испытания собственных интеллектуальных способностей; б) из азартно-корыстных соображений; в) ради игрового удовольствия. В структуре игрового влечения автор выделяет два уровня: а) осознаваемый, требующий напряжения умственной активности, тактических навыков, упорства, граничащего с параноя льностью, и б) бессознательный, в рамках которого игрок, даже не желая этого, приобретает стереотипные поведенческие навыки и эмоциональные реакции.

Автор приходит к выводу, что прогноз о возможности совершения игроком компьютерного преступления должен основываться на соотношении негативной и позитивной направленности его личности. Качественное выражение этого соотношения характеризует

криминогенность личности, которой присущ определенный процесс становления. Одной из составляющих этого процесса названо привыкание к компьютерным играм и трансформация в соответствующий поведенческий тип, при котором условия конкретного причинения становятся таковыми при приобретении определенной качественной меры.

Пятый параграф второй главы «Виктимологические аспекты компьютерной преступности» посвящен изучению взаимосвязи поведения лица, совершившего компьютерное преступление, с поведением его жертвы или с её особыми личностными качествами.

Компьютерные преступления характеризуются не только определенной скрытностью преступных деяний, но и виктимо-анонимностью жертв. При их совершении отсутствует прямой контакт с жертвой, которая является обезличенной, неперсонифицированной для компьютерного преступника, поскольку посягательство совершается опосредованно – с помощью ЭВМ.

По мнению диссертанта, жертвы компьютерных преступлений – это субъекты информационного обмена, с одной стороны, непосредственно пострадавшие от преступления, независимо от того, признаны формально потерпевшими или нет, а с другой – являющиеся носителями реализованной виктимности. Результаты проведенного исследования позволили автору выделить в их числе физических лиц и определенные общности людей в разной степени интеграции. К последним отнесены юридические лица независимо от формы собственности; общественные организации; церковные организации; малые неформальные социальные группы, объединившиеся по интересам; общество и государство в случае причинения вреда общественным интересам или интересам национальной безопасности. Традиционные типы потерпевших: нейтральный и некритичный применительно к компьютерным преступлениям дополнен «патологическим» типом, к которому отнесены лица, чье поведение определяется личностными психологическими особенностями,

обусловленными патологической компьютерной зависимостью, неболезненными формами пристрастия к компьютерным играм или пребыванию в Internet.

Автором в виктимологических рамках рассмотрены не только психологические личностные свойства жертв – физических лиц, но и факторы, связанные с особенностями социализации их личности, факторы социального характера, относящиеся к положению жертвы в социальной иерархии общества, поведенческие (деятельностные), провоцирующие возможность совершения компьютерных преступлений. Они рассмотрены как единый причинно связанный процесс, находящийся, если не в прямой зависимости с преступлением, то в определенной опосредованной связи.

Автор полагает, что состояние определенной личностной уязвимости может остаться гипотетической и «не востребованной», а может быть реализованной преступным посягательством. Ход развития этого процесса зависит как от объективных, так и от субъективных факторов, которые могут предопределить характер виктимного поведения жертвы в период, непосредственно предшествующий преступному посягательству. При этом обращается внимание на определенную техническую уязвимость компьютерных технологий и самих компьютеров.

По мнению автора, вероятность стать жертвой компьютерного преступления может постоянно увеличиваться, если не будут разрабатываться и реализовываться на практике соответствующие предупредительные меры и, самое главное, – их правовая обеспеченность.

В третьей главе «Проблемы уголовно-правовой защиты сферы компьютерной информации», состоящей из четырех параграфов, уточнены уголовно-правовые признаки преступлений в сфере компьютерной информации в целях четкого законодательного определения их составов, единообразного правоприменения и выработки соответствующих уголовно-правовых мер защиты охраняемой законом компьютерной информации. Автор обращается к анализу тех признаков

составов преступлений, которые вызывают споры в теории и осложнения при практическом применении.

Первый параграф третьей главы «Особенности объекта преступлений в сфере компьютерной информации» посвящен анализу основных общетеоретических предпосылок классификации социальных объектов. Автор не только рассматривает высказанные в литературе мнения, посвященные анализу объекта преступлений в сфере компьютерной информации и их классификации, но и предлагает собственный аргументированный подход к этой проблеме.

Основываясь на господствующей в теории отечественного уголовного права концепции, согласно которой общим объектом преступлений признаются общественные отношения, охраняемые уголовным законом, диссертантом разработаны предпосылки определения родового, видового и непосредственных объектов преступлений в сфере компьютерной информации, определены их понятия и раскрыто содержание. В частности, указывается, что соотношение понятий родового и видового объектов для данной группы преступлений свидетельствует о необходимости детализации понятия общественной безопасности в части выделения отношений информационной безопасности. Понимая под родовым объектом отношения общественной безопасности в целом, в качестве видового объекта выделяются общественные отношения по правомерному и безопасному использованию, хранению, распространению и защите компьютерной информации, автоматизированных систем обработки информации**,** необходимых для нормальной жизнедеятельности общества в целом. Иными словами – это отношения безопасности информации и информационных систем от угроз несанкционированного и неправомерного воздействия посторонних лиц.

Исходя из теоретического догмата о том, что непосредственным объектом является отдельно взятое общественное отношение, сущность которого состоит в охране уголовно-правовой нормой возможности

действовать определенным образом или пребывать в известном состоянии, сформулировано его понятие применительно к каждому составу преступлений, входящих в главу 28 Уголовного кодекса РФ, и уточнен перечень общественных отношений, могущих выступающих в качестве факультативного непосредственного объекта (в сфере охраны личных прав и свобод, экономики и экономической деятельности, здоровья населения и общественной нравственности, государственной власти).

Учитывая, что компьютер и компьютерная информация (в таких формах, как цифровая, сжатая, зашифрованная) представляет собой особую материю, а нарушение охраняемых уголовным законом общественных отношений происходит посредством посягательства на компьютерную информацию, рассмотрено соотношение объекта и предмета преступлений в сфере компьютерной информации. Исходя из того, что как научная категория информация представляет собой многоаспектное явление, понятие «информация» проанализировано в философском понимании, в социальном ракурсе, с позиций кибернетики, в техническом аспекте и в уголовно-правовом смысле. Приведены виды информации, изложена авторская классификация социальной информации.

Диссертант констатирует, что в качестве предмета преступления в сфере компьютерной информации могут выступать банки данных, различные компьютерные программы, компьютеризованные объекты авторского права и т. д. *(«пассивная информация»)*. В случаях, когда использование компьютерной информации носит активный характер, она выступает в качестве орудия совершения преступления *(«активная информация»)* и с её помощью осуществляется воздействие на «пассивную информацию». В качестве «активной информации» могут выступать компьютерные команды, «вирусные» компьютерные программы.

В описании предмета преступного посягательства законодатель использует разные формулировки: «охраняемая законом компьютерная информация» (ст. 272 УК), «информация» (ст. 273 УК), «охраняемая

законом информация ЭВМ» (ст. 294 УК). Автор считает, что данные термины используются законодателем в Уголовном кодексе как синонимы. Признак охраняемости законом вытекает из правового режима информации, который охарактеризован в работе следующими составляющими: 1) свободное пользование открытой информацией; 2) право собственности (законного владения) на информацию; 3) категорийность информации по доступу к ней; 4) законодательная определённость в порядке уголовно-правовой защиты информации.

Исходя из этих позиций, в параграфе формулируется определение понятия объекта и предмета преступного посягательства применительно к статьям 272–274 УК РФ. В связи с законодательным отнесением компьютерной информации к объектам авторского права делается вывод о необходимости обязательной защиты нарушенных прав собственника информации или законного владельца (за исключением случаев, прямо указанных в законе) в форме гражданского иска по соответствующим уголовным делам.

Второй параграф третьей главы «Объективная сторона преступлений в сфере компьютерной информации» посвящен рассмотрению объективной стороны всех составов преступлений в сфере компьютерной информации по УК РФ.

Деяние как обязательный признак составов рассматриваемых преступлений охарактеризовано на основе анализа уголовного законодательства, судебной практики и высказанных в юридической литературе точек зрения. Выделены общественно опасные деяния, осуществляемые без использования компьютерных устройств в качестве способа проникновения в информационные системы или воздействия на них и с их использованием. В работе обоснована целесообразность понимания неправомерного доступа к компьютерной информации в смысле ст. 272 УК как несанкционированное собственником информации (или законным владельцем) ознакомление лица с данными,

содержащимися на машинных носителях, в ЭВМ, системе ЭВМ или их сети. В смысле ст. 274 УК – как нарушение установленного и зафиксированного собственником информации порядка взаимодействия с ЭВМ, системой ЭВМ или их сетью.

С позиции специфики данных преступных деяний и возможности причинять вред не только информационным отношениям последствия преступлений в сфере компьютерной информации разделены: а) на материальный вред в виде реального уменьшения имущества собственника (законного владельца) информации либо упущенной выгоды, размер которого может выражаться в виде крупного или значительного материального ущерба; б) физический вред в виде причинения смерти или различной тяжести вреда здоровью человека; в) моральный вред, при определении которого необходимо исходить из субъективной оценки потерпевшим тяжести причиненного ему нравственного ущерба и объективных данных.

Причинная связь между неправомерным и общественно опасным деянием и наступившими в результате общественно опасными последствиями в преступлениях в сфере компьютерной информации с материальными составами определяется как объективная связь между деянием и последствием, при которой деяние предшествует последствию во времени и представляет собой необходимое, закономерное и решающее условие его наступления. Анализ характера причинной связи в рассматриваемых составах свидетельствует о её двояком характере: может быть прямой (ст. 272 УК) или осложненной вмешательством дополнительных факторов (ст. 274 УК).

Автор, исследовав практику применения уголовно-правовых норм, содержащихся в главе 28 УК РФ, пришел к выводу, что основные проблемы правоприменения связаны с различным пониманием бланкетных диспозиций; сложностью определения оценочных признаков; отсутствием единого мнения относительно понятийного аппарата, характеризующего

диспозиции уголовно правовых норм; отсутствием опыта применения законодательных новелл и официальных разъяснений законодательства в сфере компьютерной информации со стороны управомоченных на то органов.

Все это побудило автора сформулировать конкретные предложения по совершенствованию уголовного законодательства, в частности внесение изменений в редакцию ст. 273 УК РФ; части 2 ст. 274 УК; дополнение статьи 242.1 УК РФ частью третьей и статьи 20 УК РФ; дополнение главы 28 УК РФ новыми составами:

Ст. 272.1 «Мошенничество с использованием компьютерных технологий».

Мошенничество с использованием компьютерных технологий – завладение чужим имуществом или правом на него, а также неправомерное извлечение иной экономической выгоды путем любого ввода, изменения, удаления, блокирования или иного неправомерного воздействия на результаты процесса обработки компьютерных данных либо любого вмешательства в функционирование компьютерной системы.

Ст. 272.2 «Подлог с использованием компьютерных технологий».

Подлог с использованием компьютерных технологий – преднамеренный ввод, изменение, стирание или блокирование компьютерных данных, влекущих за собой нарушение их аутентичности, в целях восприятия использования последних в юридических целях в качестве изначальных.

Третий параграф третьей главы «Субъективная сторона преступлений в сфере компьютерной информации» посвящен анализу субъективных признаков применительно к каждому составу преступлений.

Субъективная сторона преступлений в сфере компьютерной информации характеризуется как такое психическое отношение преступника к совершенному им деянию и к наступившим в результате последствиям, которое выражает преднамеренно-антисоциальное (в

умышленных преступлениях) либо безразлично-пренебрежительное (в неосторожных преступлениях) отношение виновного к охраняемым уголовным законом интересам личности, общества и государства в информационной сфере.

Исследователи единодушны в понимании вины при неправомерном доступе к компьютерной информации в форме прямого или косвенного умысла, что нельзя сказать об исследованиях субъективной стороны состава преступления, предусмотренного ст. 273 УК РФ. Автор, анализируя высказанные в литературе позиции, приходит к выводу, что заведомость знаний о свойствах создаваемой компьютерной программы (или вносимых изменений в существующую программу для ЭВМ) для виновного лица означает как достоверность знания о возможных вредоносных последствиях таких программ, так и наличие только собственной осведомлённости, что идентично желанию в материальных составах, и что характеризует форму вины.

При характеристике субъективной стороны состава преступления, предусмотренного ст. 274 УК РФ, автор рассматривает высказанные в литературе мнения по этому вопросу и аргументирует позицию, согласно которой законодатель связывает осознание виновным лицом общественной опасности совершаемого нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, противоправности деяния и зависимости между их нарушением и наступлением существенного вреда. При этом обращается внимание на то, что четкое представление о правилах, нарушение которых может повлечь привлечение к уголовной ответственности, имеет принципиальное значение для квалификации содеянного. Автор подразделяет их на группы: а) правила, устанавливаемые изготовителями ЭВМ (правила технической эксплуатации), б) правила, устанавливаемые разработчиками компьютерных программ (правила работы с программами), в) правила, устанавливаемые владельцами (законными пользователями) ЭВМ, системы или сети ЭВМ.

В работе отмечается, что мотив и цель совершения преступлений в сфере компьютерной информации, не являясь конструктивным признаком субъективной стороны, не влияют на квалификацию содеянного, но учитываются судом при индивидуализации наказания и являются необходимым условием для выработки обоснованных и эффективных мер противодействия совершению компьютерных преступлений. Диссертантом они связываются с индивидуальными и социально-психологическими свойствами различных преступников (исследовательский интерес, хулиганские побуждения, месть, интеллектуальный вызов, безответственность, самоутверждение), с особенностями способов совершения преступлений (корыстные побуждения, политические цели, нанесение ущерба авторским правам, вандализм, шпионаж), с болезненными или пограничными отклонениями в психике (компьютерные фобии, игровой мотив).

Четвертый параграф третьей главы «Субъект преступлений в сфере компьютерной информации» посвящен исследованию уголовно-правовых признаков субъекта преступлений как одного из обязательных элементов состава преступлений в сфере компьютерной информации.

В работе обращается внимание на возможность обладания субъектов преступлений в сфере компьютерной информации, наряду с общими, дополнительными признаками, наличие которых переводит их в разряд специальных субъектов. Посредством вычленения из законодательных формулировок конкретных составов преступлений и их синтезирования в диссертации представлена классификация субъектов преступлений в сфере компьютерной информации. Подвергнута критической оценке позиция тех авторов, которые пытаются ограничить круг возможных субъектов неправомерного доступа к компьютерной информации. Предложен собственный аргументированный подход к этой проблеме и очерчен круг лиц, обладающих правом доступа к ЭВМ, системе ЭВМ или их сети.

Использование лицом своего служебного положения при совершении посягательства в сфере компьютерной информации рассмотрено диссертантом в двух плоскостях: в «узком смысле» как противоправные деяния в пределах служебной компетенции лица, в рамках предоставленных ему прав и полномочий, возложенных законами, инструкциями, уставами, функциональными обязанностями, и в «широком смысле», как действия вне служебных рамок, обусловленные «авторитетом» либо «влиянием должности». С учетом изложенного, сформулирован круг лиц, которые могут осуществить неправомерный доступ к охраняемой законом компьютерной информации, используя свое служебное положение.

В работе обращается внимание на необходимость в процессе планирования предупредительных мер учитывать характеристики не только субъектов компьютерных преступлений, но и особенности внутренних пользователей, которые могут представлять угрозу конфиденциальности компьютерной информации. Так, большинство злоупотреблений в финансовой сфере, связанных с нарушениями в области компьютерной информации, происходит при прямом или косвенном участии сотрудников: в связи с ошибками персонала – 55 %; в связи с защитой информации – 20%; из-за действий обиженных сотрудников – 9%; из-за внешнего нападения – 1-3% и др. На основании выделения в зависимости от сфер деятельности видов угроз, исходящих от персонала, внутренние пользователи подразделены на «группы риска».

Основываясь на том, что изучение компьютерной грамотности с раннего школьного возраста позволяет ребенку осознавать общественную опасность совершаемых им деяний в информационной сфере, автор высказывает мнение о возможности предусмотреть уголовную ответственность для лиц, достигших ко времени совершения преступления 14 лет, за создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ).

В четвертой главе «Актуальные направления противодействия компьютерной преступности», состоящей из четырех параграфов, сформулировано понятие противодействия компьютерной преступности; изложена система мер противодействия, что позволило дифференцировать пласты исследования на концептуальный, законодательный и организационный. Определены основные направления международного сотрудничества России в данной области.

Первый параграф четвертой главы «Противодействие компьютерной преступности как социально-правовая функция государства» посвящен осмыслению вопросов, обусловленных необходимостью обеспечения безопасности социальных процессов.

Подчеркнуто, что анализ современного состояния компьютерной преступности, выявление её причинного комплекса, изучение личности преступника не является самоцелью, а выступает условием и предпосылкой разработки мер противодействия ей. В условиях всеобщей компьютеризации потребность в защите информации трансформировалась в глобальную проблему, а противодействие компьютерной преступности – в деятельность, с одной стороны, направленную на сокращение преступлений, известных материальному праву (прикладной аспект), с другой стороны - на преступность в информационной сфере как на социальное явление со сложным причинно-следственным комплексом (общесоциальный аспект). Такой подход позволил диссертанту рассматривать противодействие как особый вид деятельности в области социального управления, призванного в рамках социально-правовой функции государства планомерно влиять на общество путем поддержания в нем нормативного порядка (средствами позитивного и репрессивного правового контроля) и минимизации девиантного поведения.

В работе с философских, общетеоретических и прикладных позиций рассмотрено понятие социального контроля, представляющего совокупность процессов в социальной системе (обществе, социальной

группе, организации и т. п.), посредством которых обеспечивается следование определенным «образцам» деятельности, а также соблюдение ограничений в поведении, нарушение которых отрицательно сказывается на функционировании системы. Характеристика криминологического содержания социального контроля позволила диссертанту сделать заключение о его ориентированности на широкую социальную превенцию, необходимости целенаправленного влияния общества на все формы девиантного поведения индивида в информационной сфере и переосмысления взаимодействия государства в лице его соответствующих органов и институтов с общественностью в решении превентивных задач. В качестве концептуальных выдвинуты такие задачи, как реальное представительство общественных субъектов в социальной превенции всех форм негативно отклоняющегося (девиантного) поведения; создание условий для формирования гражданского общества как одного из инструментов в обеспечении правопорядка в обществе; выстраивание реальной иерархии правоохраняемых ценностей на основе согласования права и нравственности; построение системы превентивных мер.

В заключении диссертантом делается вывод о том, что противодействие компьютерной преступности является не просто особым видом деятельности в области социального управления, призванным влиять на поведение индивидуумов в информационной сфере и направленным на сокращение предусмотренных материальным правом преступлений. Содержательная составляющая этой деятельности формируется в рамках социально-правовой функции государства с позиции комплексного подхода, при котором охватываются различные отрасли права с учетом их междисциплинарных связей (в рамках правового контроля) в сочетании с иными социально значимыми факторами, а сама деятельность выходит за пределы системы правоохранительных органов.

Второй параграф четвертой главы «Понятие, содержание и формы

противодействия компьютерной преступности» посвящен рассмотрению понятия «противодействие» в общесоциальном и специально-криминологическом аспектах на основе знания причин и условий, способствующих совершению преступлений в сфере компьютерной информации, с целью опережения их действия.

Автором отмечается, что целенаправленное воздействие государства и общества на факторы, сопутствующие противоправному поведению в информационной сфере, возможно, в первую очередь, посредством совокупности методов и средств различных отраслей права в рамках правового контроля, который подразделен на два вида: позитивный и репрессивный. При этом указывается, что возможности криминального цикла (уголовного, уголовно-процессуального, уголовно-исполнительного законодательства) должны сочетаться с нормами гражданско-правового цикла. В работе осуществлен подробный анализ позитивного правового контроля, нацеленного на создание определенного правового режима в информационной сфере и условий правомерного использования информационного продукта, средствами конституционного, международного, информационного, гражданского и административного права. Анализ репрессивного правового контроля над компьютерной преступностью, обеспечиваемого нормами уголовного и уголовно-процессуального права, осуществлен посредством рассмотрения их превентивной роли.

Диссертантом дается общая характеристика криминологического законодательства России, регулирующего информационные отношения, и обращается внимание на необходимость разработки основополагающего законодательного акта, как, например, Основы федерального законодательства Российской Федерации о социальном контроле преступности.

В заключении формулируется вывод о необходимости осознания того факта, что контролировать поведение пользователей ЭВМ, систем

ЭВМ или их сети посредством одних законодательных санкций практически невозможно. Необходимо сочетание средств позитивного и репрессивного правового контроля с реализацией комплекса государственных мер социально-экономического, политического и организационного характера, обеспечивающих доминирующую роль законности в обществе в целом и в информационной сфере в частности.

Третий параграф четвертой главы «Комплексная система мер противодействия компьютерной преступности» посвящен характеристике мер противодействия компьютерной преступности с позиции построения целостной системы и её эффективного практического функционирования.

Разработка такой системы осуществлена в рамках единых принципов, среди которых выделены законность, демократизм, комплексность, масштабность и целенаправленность. Автор подробно их анализирует, исходя из того, что они должны использоваться при подготовке конкретных мероприятий по устранению причин и условий, способствующих совершению компьютерных преступлений; выступать в качестве основополагающих при формулировании предупредительных мер; являться фундаментом построения правовых основ противодействия компьютерной преступности. Необходимость рассмотрения теоретических основ противодействия компьютерным преступлениям обоснована также наличием проблемных вопросов, перечень которых обозначен в работе самостоятельно.

Раскрытие теоретических основ рассматриваемой проблемы позволило диссертанту сформулировать модель процесса построения системы мер противодействия, в основу которого положен постоянный мониторинг изменений социальной среды, происходящих под воздействием процесса компьютеризации. При этом обращается внимание на тот факт, что компьютерного преступника формирует не только социальная, но и виртуальная среда, которая подменяет человеческое

общение на общение виртуальное. Поэтому при выработке предупредительных мер этот аспект необходимо учитывать и предусматривать меры воздействия на факторы предрасполагающего виртуального воздействия, которые также могут формировать криминогенные свойства личности.

Спектр практических мер противодействия компьютерной преступности сформулирован в рамках комплексного подхода, при котором охватывается все многообразие криминогенных факторов (правовых, экономических, политических, психологических, воспитательных и др.), а сами меры направлены на социальную, личностную и ситуативную сферы бытия человека и ориентированы на пользователей ЭВМ, систем ЭВМ или их сети, которые не совершали противоправных деяний, но находятся в неблагоприятных условиях и под их влиянием могут совершить такие деяния, или ранее совершали компьютерное преступление и подвергались мерам уголовно-правового воздействия.

Сформулирован двойственный подход к содержательному наполнению мер противодействия компьютерной преступности, которые, с одной стороны, направлены на сокращение преступлений в сфере компьютерной информации, известных уголовному праву, с другой – на нейтрализацию негативных криминальных процессов в информационной сфере общества. Указано, что на практике меры противодействия могут носить *фрагментарный характер*, обеспечивая избирательность относительно конкретной угрозы и локальность методов защиты против несанкционированного доступа, и *комплексный характер*, объединяя разнородные меры противодействия угрозам несанкционированного доступа. Автор излагает имеющиеся в литературе классификации групп указанных мер и констатирует их различие только в терминологическом плане и в уровне обобщения. Исходя из результатов анализа причинного комплекса и с учетом технических особенностей совершения

преступлений в сфере компьютерной информации, автор предлагает собственную систему мер организационно-управленческого, кадрового, технического и правового обеспечения, сформулированную индивидуально в рамках отдельного объекта защиты.

Диссертантом формулируется общий алгоритм системы безопасности ЭВМ, системы ЭВМ или их сети. Предлагается на отдельно взятом объекте информационного обмена противодействовать криминальным атакам на охраняемую законом компьютерную информацию посредством разработки и реализации алгоритма безопасности ЭВМ в рамках интегрированной системы, объединяющей многообразие средств защиты на основе единого программно-аппаратного комплекса с общей информационной средой и единой базой данных. При этом указывается, что, обладая высокой надежностью за счет взаимодополнения и резервирования технических средств, такая система может обеспечить реальную защиту ЭВМ, системы ЭВМ или их сети, только в сочетании со стойким персоналом сотрудников. По мнению автора в условиях, когда информационное пространство перерастает в гуманно компьютеризированное общество будущего, пользователь ЭВМ должен быть отягощен моральным долгом и профессиональной этической ответственностью.

В итоге делается вывод о том, что система мер противодействия компьютерной преступности должна отвечать не только общим требованиям законности, демократизма, гуманизма, учета территориальности и отраслевых условий, системности, объективности, конкретности, но и специфическим требованиям, среди которых выделены правовая и информационная обеспеченность, социально-экономическая обоснованность, эффективность и скоординированность.

Четвертый параграф четвертой главы «Основные направления международного сотрудничества России в области противодействия компьютерной преступности» посвящен рассмотрению международного

сотрудничества в сфере противодействия преступности в двуединстве: как деятельность и как международный принцип, при акцентировании внимания на деятельностном аспекте.

В работе отмечается, что государство в рамках общей стратегии информатизации общества, направляя усилия на решение триединой задачи: формирование информационной среды общества; развитие информационного сервиса услуг, создание организационно-правовых основ безопасности компьютерной информации – сталкивается с проблемами межгосударственного взаимодействия, решение которых в совокупности с комплексом внутригосударственных мер повысит эффективность противодействия компьютерной преступности.

Исходя из отсутствия единообразного подхода к определению форм международного сотрудничества, анализируются высказанные в литературе различные позиции по данному вопросу и формулируется собственная классификация форм международного сотрудничества в зависимости от характера критерия, положенного в основу такого сотрудничества, а именно: в зависимости от содержания международного сотрудничества; характера преступности; общественной опасности и распространенности отдельного вида преступлений; структуры механизма международного сотрудничества.

С позиции практического осуществления международное сотрудничество в сфере противодействия преступности рассматривается в рамках двух основных общепризнанных форм: а) международных соглашений и б) международных органов и организаций. В работе дается подробная характеристика каждой формы международного сотрудничества применительно к противодействию компьютерным преступлениям, формулируются основные направления деятельности, излагается практическая составляющая Организации Объединенных Наций и Международной организации уголовной полиции (Интерпол).

Анализ организационных форм и имеющих место проблем международного сотрудничества приводит диссертанта к выводу о необходимости разработки и принятия комплексной межгосударственной программы противодействия компьютерной преступности, основанной на Конвенции о киберпреступности и предусматривающей два уровня — международный и внутригосударственный, подробная характеристика которых дается в работе.

В заключении работы в синтезированном и сконцентрированном виде сформулированы обобщающие, наиболее значимые результаты исследования, подводящие итог выводы и предложения: теоретические положения, характеристики, определения, рекомендации по применению действующего уголовного законодательства в сфере компьютерной информации и предложения по его совершенствованию для использования в правотворческой деятельности, а также комплексная система мер противодействия компьютерной преступности.

Сделан вывод о том, что в основе современного общества лежат информация, информационные и телекоммуникационные технологии, противоправное использование которых на базе существующих в обществе противоречий и с учетом индивидуально-личностных особенностей компьютерных преступников порождают прогрессирующее развития компьютерной преступности как социального явления.

Изложена криминологическая характеристика компьютерной преступности как совокупность наиболее характерной криминологически значимой взаимосвязанной информации о признаках и свойствах данного вида преступлений, личности компьютерного преступника, причинах и условиях их совершения, основных направлениях предупредительной деятельности. Очерчены особенности компьютерной преступности, которая, являясь составной частью общей преступности, порождается как общими социальными противоречиями, так и специфическими особенностями информационной сферы.

Отмечено, что осуществляемая предупредительная деятельность нуждается в комплексном подходе к формированию основополагающих начал сдерживания компьютерной преступности на социально нейтральном уровне и форм их достижения, ориентированных на перспективу построения информационного общества на географическом пространстве Российской Федерации. Констатировано, что противодействие компьютерной преступности – это многоуровневый, сложный и дорогостоящий процесс, связанный с комплексными решениями, рассчитанный на длительный период времени, широкий круг субъектов предупредительной деятельности, ориентированный на широкую социальную превенцию, охват новых форм девиантного поведения, механизм регулирования которого включает правовые нормы, нормы морали, корпоративные и этические нормы поведения, учитывающий перспективы развития международного сотрудничества на глобальном и региональном уровнях.

Основные положения диссертации отражены в 42 работах, из них 2 монографии, 6 учебных пособий, 34 научных статьи, из которых 10 опубликовано в журналах перечня ВАК России.

Монографии и учебные пособия

1. *Лопатина Т. М.* Компьютерная преступность: национальный опыт борьбы и международное сотрудничество. Монография. – Смоленск: Универсум, 2005. – 17,5 п.л. / Рецензия на монографию. Современное право. 2006. № 4.
2. *Лопатина Т. М.* Компьютерная преступность и противодействие ей: Монография. – Смоленск: Универсум, 2006. – 11,5 п. л.
3. *Лопатина Т. М.* Основы компьютерной безопасности Республики Казахстан. – Петропавловск: СКЮА, 1999. – 2,8 п. л.
4. *Лопатина Т. М.* Вопросы квалификации отдельных составов преступлений со специальным субъектом: Учебное пособие. – Петропавловск: СКЮА, 2002. – 6,7 п. л.

5. *Лопатина Т. М.* Преступления в сфере компьютерной информации по законодательству Республики Казахстан. – Казахский гуманитарный юридический университет, 2002. – 2,0 п. л.
6. *Лопатина Т. М.* Проблемы компьютерной преступности. Авторский курс лекций: Учебное пособие. – Петропавловск: СКЮА, 2003. – 11,1 п. л.
7. *Лопатина Т. М.* Основные направления противодействия компьютерной преступности: Учебное пособие. – Смоленск: Универсум, 2005. – 5,0 п. л.
8. *Лопатина Т. М.* Уголовно-правовая защита компьютерной информации: Учебное пособие. – Смоленск: Универсум, 2006. – 4,6 п. л.

Научные статьи, опубликованные в периодических изданиях перечня ВАК:

9. *Лопатина Т. М.* Терроризм и информационные технологии // Современное право. 2005. № 1. – 0,5 п. л.
10. *Лопатина Т. М.* Международный опыт правового обеспечения информационной безопасности // Современное право. 2005. № 2. – 0,5 п. л.
11. *Лопатина Т. М.* Место латентности в структуре компьютерной преступности // «Черные дыры» в российском законодательстве. 2005. № 3. – 0,5 п. л.
12. *Лопатина Т. М.* Теоретические основы и социальная обусловленность профилактики латентной компьютерной преступности // Бизнес в законе (Приложение к журналу «Черные дыры» в российском законодательстве). 2005. № 3. – 0,5 п. л.
13. *Лопатина Т. М.* Ретроспектива формирования самостоятельного правового института компьютерных преступлений // Человек. Преступление и наказание. 2005. № 4. – 0,5 п. л.
14. *Лопатина Т. М.* Виктимологическая профилактика преступлений в сфере компьютерной информации // Современное право. 2005. № 7. – 0,5 п. л.

15. *Лопатина Т. М.* Отдельные проблемные вопросы характеристики уголовно-правовых признаков субъекта преступлений в сфере компьютерной информации // Российский судья. 2006. № 1. – 0,4 п. л.
16. *Лопатина Т. М.* Не пора ли дополнить уголовный кодекс новыми составами компьютерных преступлений? // Современное право. 2006. № 4. – 0,3 п. л.
17. *Лопатина Т. М.* Виктимологическая профилактика компьютерной преступности // Российская юстиция. 2006. № 4. – 0, 5 п. л.
18. *Лопатина Т. М* Противодействие преступлениям в сфере компьютерной информации (правоприменительный аспект) // Законность. 2006. № 6. – 0,3 п. л.

Иные научные статьи и публикации:

19. *Лопатина Т. М.* Комплексная оценка качества обучения в условиях применения информационных и телекоммуникационных технологий // Университеты и региональное развитие. Материалы II Международной научно-практической конференции. – Смоленск: Универсум, 2002.–0,4 п.л.
20. *Лопатина Т. М.* Internet – государство без границ // Актуальные проблемы реформирования правовой системы Республики Казахстан. Материалы III Международной научно-практической конференции. – Петропавловск: СКЮА, 2003. – 0,4 п. л.
21. *Лопатина Т. М.* Профессиональная этика как одно из условий безопасности информационных технологий // Актуальные проблемы правовой культуры: Сборник межвузовской научной конференции. – Смоленск: Универсум, 2004. – 0,4 п. л.
22. *Лопатина Т. М.* Информационная безопасность в компьютерных сетях // Университетский вестник. – Смоленск: СГУ, 2004. – 0,4 п. л.
23. *Лопатина Т. М.* Современные представления о криминалистической характеристике транснациональных компьютерных преступлений и возможности использования её данных в процессе их раскрытия и

расследования // Правовая реформа в Республике Казахстан: проблемы и перспективы. Материалы IV Международной научно-практической конференции. – Петропавловск: СКЮА, 2004. – 0,4 п. л.

24. *Лопатина Т. М.* Криминологическая характеристика и отдельные аспекты профилактики преступности несовершеннолетних в информационной сфере // Творческое наследие В. И. Чаславского и современность. Материалы научно-практической конференции. – Смоленск, 2004 – 0,4 п.л.
25. *Лопатина Т. М.* Правовая культура молодежи как фактор профилактики преступности в информационной сфере // Профилактика безнадзорности и правонарушений несовершеннолетних. Материалы Всероссийской научной конференции. – Смоленск: СГПУ, 2004. – 0,4 п. л.
26. *Лопатина Т. М.* Некоторые аспекты проблемы моральной ответственности компьютерных систем // Научные труды. Российская академия юридических наук. Выпуск 4. В трех томах. Т. 1. – М.: Издательская группа «Юрист», 2004. – 0,5 п. л.
27. *Лопатина Т. М.* Отдельные криминологические тенденции воспроизводства преступлений в сфере компьютерной информации // Правовые и организационно-тактические меры борьбы с незаконным оборотом наркотиков. Материалы научно-практической конференции. – Смоленск: Смоленский регион IPA, 2005 г. – 0,5 п.л.
28. *Лопатина Т. М.* Вопросы институализации правонарушений в сфере компьютерной информации // X Кирилло-мефодиевские чтения. Материалы научно-практической конференции. – Смоленск, 2005.– 0,5 п.л.
29. *Лопатина Т. М.* Некоторые аспекты проблемы унификации информационного законодательства стран СНГ (на примере Российской Федерации, Республики Беларусь и Республики Казахстан) // Унификация законодательства стран СНГ: состояние и перспективы развития. Материалы научно-практической конференции. – Смоленск: «Универсум», 2005. – 0,5 п. л.

30. *Лопатина Т. М.* Всеобщая информатизация общества как один из факторов воспроизводства преступлений в сфере компьютерной информации // Современные наукоемкие технологии. 2005. № 3. – 0,2 п. л.

31. *Лопатина Т. М.* Некоторые аспекты проблемы моральной ответственности компьютерных систем // Правовые вопросы связи. 2005. № 1. – 0,4 п. л.

32. *Лопатина Т. М.* К вопросу о месте норм о компьютерных преступлениях в системе уголовного законодательства // Вестник Академии права и управления. 2005. № 5. – 0,4 п. л.

33. *Лопатина Т. М., Фурдей Г.А.* Транснациональный характер компьютерной преступности // Сборник научных трудов. Выпуск 5. – М.: РИПО ИГУМО. – 2005. – 0,7/0,5 п. л.

34. *Лопатина Т. М.* Современные тенденции причинного комплекса преступлений в сфере компьютерной информации // Информатизация и информационная безопасность правоохранительных органов. Материалы XIV международной научной конференции. – М.: Академия управления МВД России, 2005. – 0,4 п. л.

35. *Лопатина Т. М.* Теоретические проблемы транснациональной компьютерной преступности // Научные труды. Российская академия юридических наук. Выпуск 4. Т. 3. – М.: Юрист, 2005. – 0,5 п. л.

36. *Лопатина Т. М.* Компьютеризация как предпосылка компьютерной преступности // Конституционная реформа в Республике Казахстан: перспективы развития. Материалы V Международной научно-практической конференции. – Петропавловск: СКЮА, 2005. – 0,7 п. л.

37. *Лопатина Т. М.* Индивидуально-психологические причины компьютерных преступлений // Актуальные проблемы современного права. – Смоленск: Универсум, 2005. – 0,5 п. л.

38. *Лопатина Т. М.* Отдельные теоретические вопросы формирования правовых институтов в современных условиях общественного развития // Университетский Вестник. – 2005. – № 3 (10). – 0,5 п. л.

39. *Лопатина Т. М.* Общесоциальные причины компьютерной преступности // Конституционная реформа в Республике Казахстан: перспективы развития. Материалы V Международной научно-практической конференции. – Петропавловск: СКЮА, 2005. – 0,5 п. л.

40. *Лопатина Т. М.* Социокультурная среда как один из факторов формирования морали информационного общения // Третьи Авраамиевские чтения. Материалы Всероссийской научно-практической конференции (1-2 ноября 2005 г.). – Смоленск: СГУ. – 0, 25 п. л.

41. *Лопатина Т. М.* Виктимологическая обусловленность компьютерной преступности // Сборник научных трудов. Выпуск 5. – М.: РИПО ИГУМО. – 2005. – 0,7 п. л.

42. *Лопатина Т. М.* Хакер – преступник или компьютерный талант? // Проблемы формирования правового государства. Материалы межвузовской научно-практической конференции. – Смоленск, 2005. – 0, 3 п. л.

Подписано в печать _____ 2006 г. Формат 60x84 1/16 Заказ №
Тираж ___ экз. Печ. л.

Отпечатано на УОП РИО ВНИИ МВД России