На правах рукописи

Тропина Татьяна Львовна

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, СОСТОЯНИЕ, УГОЛОВНО-ПРАВОВЫЕ МЕРЫ БОРЬБЫ

Специальность: 12.00.08 — уголовное право и криминология; уголовно-исполнительное право

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Владивосток — 2005

Работа выполнена на кафедре уголовного права Юридического института Дальневосточного государственного университета

Научный руководитель:	доктор юридических наук, профессор **В.А. Номоконов**
Официальные оппоненты:	доктор юридических наук, профессор **С.В. Землюков**
	доктор юридических наук, доцент **С.В. Пархоменко**
Ведущая организация	Московская государственная юридическая академия

Защита диссертации состоится «4» октября 2005 г. в 14.00 часов на заседании диссертационного совета Д 212.056.01 по защите диссертаций на соискание ученой степени доктора юридических наук в Дальневосточном государственном университете по адресу: 690950, г. Владивосток, ул. Октябрьская, 25.

С диссертацией можно ознакомиться в библиотеке Юридического института Дальневосточного государственного университета.

Автореферат разослан «30» 08 2005 г.

Ученый секретарь диссертационного совета
кандидат юридических наук, доцент Т.Б.Басова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Мы живем в эпоху информационного общества, когда компьютеры и телекоммуникационные системы охватывают все сферы жизнедеятельности человека и государства. Но человечество, поставив себе на службу телекоммуникации и глобальные компьютерные сети, не предвидело, какие возможности для злоупотребления создают эти технологии. Сегодня жертвами преступников, орудующих в виртуальном пространстве, могут стать не только люди, но и целые государства. При этом безопасность тысяч пользователей может оказаться в зависимости от нескольких преступников. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете.

На XI Конгрессе ООН по предупреждению преступности и уголовному правосудию, прошедшем в апреле 2005 года, преступности, связанной с использованием компьютеров, было уделено особое внимание: этот вопрос был включен в повестку дня и рассматривался в рамках проблемы эффективных мер по борьбе с транснациональной организованной преступностью. Эксперты ООН в рекомендациях, подготовленных к XI Конгрессу, говорят об особом характере киберпреступности и необходимости применения комплексных подходов по борьбе с ней, а также о неотложных мерах по обновлению уголовного законодательства государств-участников ООН, таких как уточнение или изъятие норм, не отвечающих сложившейся ситуации, или принятие норм, касающихся новых видов киберпреступлений[1].

Бангкокская декларация, которая стала результатом деятельности XI Конгресса ООН по предупреждению преступности и уголовному правосудию, также свидетельствует об актуальности проблемы киберпреступности. В Декларации отмечается, что в период глобализации быстрое развитие информационных технологий и новых систем телекоммуникаций и компьютерных сетей сопровождается зло-

[1] См. Семинар-практикум 6: Меры по борьбе против преступлений, связанных с использованием компьютеров// материалы Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию. A/CONF.203/14. Бангкок. — 2005. — С. 25.

употреблением этими технологиями в преступных целях, а также подчеркивается необходимость разработки национальных мер и развития международного сотрудничества по противодействию киберпреступности.

Опасность киберпреступности как для всего мира, так и для России признают и российские правоохранительные органы. Так, по данным Главного управления специальных технических мероприятий МВД России, киберпреступность (преступность в сфере высоких технологий) в настоящее время является одной из наиболее серьезных угроз национальной безопасности Российской Федерации в информационной сфере[2].

К сожалению, в российской специальной литературе практически не освещена проблема киберпреступности как следствия глобализации информационных процессов. Этот пробел еще предстоит восполнить. России также не оказалось среди государств, подписавших в ноябре 2001 года Конвенцию Совета Европы о киберпреступности. И если эта конвенция является продуктом длительного труда, то есть мировое сообщество более десяти лет озабочено данной проблемой, то наша страна пока, увы, не готова ни к подписанию данной конвенции, ни к международному сотрудничеству в этой области. Но, справедливо будет упомянуть, что и международное сообщество тоже пока находится в поиске не только методов борьбы с этой проблемой, но и в процессе выработки единой политики по данному вопросу, в том числе понятийного аппарата.

Степень научной разработанности проблемы. В России в настоящее время отсутствуют фундаментальные исследования, посвященные проблеме киберпреступности как явлению, охватывающему собой весь спектр преступлений, совершаемых в глобальных информационных сетях. В основном работы российских ученых посвящены либо совершенствованию уголовной ответственности за совершение компьютерных преступлений, либо направлены на изучение криминологической характеристики компьютерной преступности в России. Исследованию киберпреступности именно как глобального явления

[2] Мирошников Б.Н. Борьба с киберпреступлениями – одна из составляющих информационной безопасности Российской Федерации [Электрон.ресурс]/ Доступно из URL: http://www.crime-research.ru/articles/Miroshl [Дата обращения: 10.11.2004 г.]

в основном посвящены работы только зарубежных ученых. В России на эту тему до настоящего времени появляются в основном научные статьи. Исключение составляет работа А.Л. Осипенко «Борьба с преступностью в глобальных компьютерных сетях: Международный опыт», анализирующая криминологические, уголовно-правовые и криминалистические аспекты проблемы преступлений, называемых автором «сетевыми»[3].

Работы зарубежных ученых: М. Бреннера и С. Гудман, Ф. Вильямса, Д. Деннинг, У. Зибера, Д. Льюиса, М. Кабэя, Б. Колина, Л. Шелли, Д. Шиндер о киберпреступности дают неплохое представление об этом явлении, но, к сожалению, указанные исследования практически никогда не охватывают Россию и российское законодательство. Тем не менее они дают хорошие теоретические основы для изучения киберпреступности в глобальном аспекте. Работы, принадлежащие перу зарубежных ученых, пока практически не переводились на русский язык, их перевод осуществлялся главным образом автором настоящего диссертационного исследования.

Изучению вопросов киберпреступности и кибертерроризма на постсоветском пространстве, а также глобальных вопросов преступности в сфере высоких технологий посвящены сборники, выпускаемые Запорожским центром исследования проблем компьютерной преступности. Также следует отметить сборники материалов научной конференции «Информационные технологии и безопасность», проходящей ежегодно на Украине, включающие в себя работы, посвященные техническим, уголовно-правовым, криминологическим, социологическим и иным аспектам киберпреступности

Уголовно-правовые и криминологические вопросы борьбы с компьютерной преступностью в отечественной науке рассматриваются также в работах В.Б. Вехова, А.Г. Волеводза, М. С. Дашяна, Б.Д. Завидова, В.Е. Козлова, В.Д. Курушина, Ю.И. Ляпунова, В.А. Мазурова, В.А.Минаева, В.Б. Наумова, В.А. Номоконова, А.Л. Осипенко, А. Г. Серго, Д. Б. Фролова, В.Н. Черкасова, В.Г. Щелкунова и др.

По теме компьютерной преступности и ответственности за совершение компьютерных преступлений выполнено несколько диссертационных исследований: С.Д. Бражника, С.Ю. Бытко, В.В. Воробьева,

[3] Осипенко А.Л. Борьба с преступностью в компьютерных сетях: Международный опыт. М., 2004.

Д.А. Зыкова, Т.П Кесареевой, В.С. Карпова, С.Г. Спириной, С.И. Ушакова[4]. Указанные диссертационные исследования, безусловно, внесли вклад в изучение компьютерной преступности в рамках Уголовного кодекса РФ, однако проблема именно киберпреступности (т.е. преступности не только компьютерной, но и любой, связанной с использованием компьютеров) комплексно и в общемировом масштабе в них не поднималась.

Существует также работа А.А. Жмыхова, посвященная изучению компьютерной преступности за рубежом, в которой исследуются проблемы этого вида преступности и ее предупреждения в зарубежных странах Вопросы борьбы с ней в Российской Федерации автором не затрагиваются[5].

Настоящая работа призвана, с учетом уже имеющихся исследований и разработок проблемы, дать определение такому явлению, как киберпреступность, отграничив его от понятия «компьютерная преступность», выявить и охарактеризовать его криминологически значимые признаки и исследовать проблемы уголовно-правовой борьбы с ним на международном и национальном уровне, в том числе в Российской Федерации.

Цели и задачи исследования. Целью настоящего исследования является изучение проблемы киберпреступности, ее криминологически значимых аспектов, необходимых для оценки степени общественной опасности этого явления, анализ мер уголовно-правовой борьбы

---

[4] Бражник, С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: дис.... канд. юрид.наук: 12.00.08. Ижевск, 2002; Бытко, С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: дис. ... канд. юрид. наук: 12.00.08. Саратов, 2002; Воробьев, В.В. Преступления в сфере компьютерной информации (Юридическая характеристика составов и квалификация): дис. ... канд. юрид. наук: 12.00.08. Н. Новгород, 2000; Зыков, Д.А. Виктимологические аспекты предупреждения компьютерного мошенничества. Автореф. дис... канд. юрид. наук: 12.00.08. Нижний Новгород, 2002; Кесареева Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет. Автореф. дис... канд. юрид. наук. Москва, 2002; Карпов, В. С. Уголовная ответственность за преступления в сфере компьютерной информации. Автореф. дис... канд. юрид. наук. Красноярск, 2002; Спирина С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации. Автореф. дис... канд. юрид. наук. Волгоград, 2001; Ушаков, С.И. Преступления в сфере обращения компьютерной информации (Теория, законодательство, практика): дис. ... канд. юрид. наук: 12.00.08. Ростов-на-Дону, 2000.

[5] Жмыхов, А. А. Компьютерная преступность за рубежом и ее предупреждение: дис. ... канд. юрид наук: 12.00.08 / А.А.Жмыхов. – М., 2003. - 178 с.

с ним и разработка предложений, направленных на повышение эффективности уголовно-правового регулирования борьбы с киберпреступностью.

Основные задачи исследования состоят в том, чтобы:

• Сформулировать понятие киберпреступности и киберпреступления, охарактеризовать виды киберпреступлений.

• Осуществить криминологический анализ состояния, структуры, динамики киберпреступности в мировом (глобальном) масштабе.

• Проанализировать правовой опыт противодействия киберпреступности на двух уровнях — международном и национальном, в том числе провести сравнительный анализ законодательства зарубежных стран.

• Через призму предмета исследования проанализировать недостатки уголовно-правовых норм, направленных на борьбу с компьютерной преступностью в Российской Федерации, и выработать предложения по совершенствованию отечественного уголовного законодательства.

Объект и предмет исследования. Объект исследования — киберпреступность, ее тенденции и особенности, а также уголовно-правовая борьба с ней.

Предметом исследования являются криминологические аспекты киберпреступности — ее состояние, структура, динамика и факторы, ее детерминирующие, вопросы уголовно-правовой борьбы с этим явлением, в том числе национальные и международные уголовно-правовые нормы, предусматривающие ответственность за деяния, совершенные в киберпространстве.

Методология и методика исследования. Методологической основой настоящей работы стал диалектический метод изучения социальных процессов и явлений. Характер поставленных исследовательских задач предопределил необходимость использования также таких методов, как сравнительно-исторический, сравнительно-правовой, метод системного анализа и конкретно-социологический метод.

Теоретическую базу исследования составили работы отечественных и зарубежных ученых С. Бреннер, В.Б. Вехова, А.Г. Волеводза, В.А. Голубева, М. Гудмана, М. С Дашяна, Д. Деннинг, Б.Д. Завидова, У. Зибера, В.Е. Козлова, А.И. Коробеева, Д. Льюиса, В.Д. Курушина, Н.А. Лопашенко, Ю.И. Ляпунова, В.А. Мазурова, В А. Минаева, В.Б. Наумова, В.А. Номоконова, А.Л. Осипенко, А Г. Серго, Д. Б. Фролова, В.Н. Черкасова, Л. Шелли, Д. Шиндер и др.

Нормативной основой работы стало международное законодательство, в том числе Конвенция Совета Европы о киберпреступности; законодательство зарубежных стран, направленное на борьбу в киберпреступностью; уголовное законодательство Российской Федерации.

Перевод зарубежной литературы и ряда норм национального законодательства стран мира с иностранных языков осуществлен автором самостоятельно.

Эмпирическую основу исследования составляют статистические данные, в том числе данные о киберпреступности, собранные международными организациями, данные обзоров компьютерной преступности США, Австралии и Великобритании, статистические и аналитические данные о компьютерной преступности в РФ и зарубежных странах. Использованы также материалы собственного исследования, в частности, интервьюирования работников правоохранительных органов и работников служб информационной безопасности и специалистов в области компьютерных технологий предприятий Приморского края (всего 110 чел.).

Научная новизна исследования заключается в том, что впервые на уровне диссертационного исследования предпринята попытка исследовать преступность, связанную с использованием компьютерных систем, в более широком, нежели это делалось ранее, аспекте. При этом компьютерная преступность рассматривается автором как составной элемент более широкого явления — киберпреступности. В диссертации дано определение киберпреступности и произведено отграничение этого понятия от понятия «компьютерная преступность». На основании криминологически значимых зарубежных и российских статистических данных исследованы общемировые тенденции киберпреступности, в том числе ее взаимосвязь с организованной преступностью. Дан обзор международных инициатив по борьбе с киберпреступностью и анализ их значимости, проанализированы основные тенденции реформирования национальных уголовных законодательств стран мира и проведен сравнительный анализ уголовно-правовых норм зарубежного законодательства, посвященных различным видам киберпреступлений. По результатам исследования сформулированы предложения по совершенствованию российского уголовного законодательства.

Теоретическая и практическая значимость исследования. Настоящее исследование восполняет пробел, образовавшийся в результате того, что рост киберпреступности опережает усилия по борьбе с ней, и способствует дальнейшему теоретическому исследованию криминологических и уголовно-правовых аспектов преступности в киберпространстве. Полученные данные и выводы могут быть использованы в учебном процессе при преподавании курса криминологии и специальных курсов.

Результаты исследования могут быть использованы также в правотворческой деятельности по совершенствованию уголовно-правовых норм об ответственности за киберпреступления.

Основные положения, выносимые на защиту.

1. Киберпреступность является объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. С ростом использования информационных технологий в различных сферах деятельности человека растет и использование их в целях совершения преступлений. Киберпреступность по своей сути гораздо шире компьютерной преступности и включает в себя целый спектр противоправных деяний.

2. Под киберпреступностью понимается совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

3. Киберпреступление — это виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству

4. Киберпреступность обладает высокой латентностью, официальная статистика правоохранительных органов не отражает достоверной картины состояния киберпреступности как на уровне государства, так и на общемировом уровне. Для оценки состояния киберпреступности необходимо использовать иные способы получения дан-

ных, такие как интервьюирование, фокусные группы, обзоры, а также метод «регистрации обращений» — виктимологический метод, заключающийся в сборе сведений о киберпреступлениях от потерпевших. Использование этих методов наряду с анализом официальной статистки позволяет исследовать масштабы кибепреступности и ее тенденции с учетом прєступлений, оставшихся за рамками зарегистрированных правоохранительными органами антиобщественных деяний.

5. Анализ криминологически значимых статистических данных свидетельствует о быстром росте киберпреступности, о возможности причинения этими преступлениями значительного финансового ущерба гражданам и организациям при минимальном риске для преступника, а также о растущей взаимосвязи киберпреступности и организованной преступности. Это свидетельствует о повышенной опасности подобного рода деяний и обусловливает необходимость реагирования на них уголовно-правовыми мерами.

6. Уголовно-правовая борьба с киберпреступностью — глобальная проблема в силу того, что киберпреступность носит трансграничный характер. Поэтому для эффективной борьбы с киберпреступлениями необходимо не только принятие соответствующих уголовно-правовых норм на национальном уровне, но и выработка единых международных стандартов, таких как определение круга деяний, подлежащих криминализации, выработка единого понятийного аппарата и единой терминологии, пересмотр существующих уголовно-правовых норм с учетом стандартов, установленных международно-правовыми документами.

7. Результаты сравнительного анализа законодательства государств мира, посвященного борьбе с киберпреступностью, показывают, что в большинстве развитых стран криминализированы в той или иной форме следующие виды деяний:

- посягательство на конфиденциальность данных,
- неуполномоченное проникновение в компьютеры и компьютерные сети,
- посягательство на конфиденциальность информации, содержащей коммерческую тайну,
- компьютерный саботаж (вмешательство в функционирование, изменение, уничтожение данных и т.п.),

- экономические киберпреступления (в частности, компьютерное мошенничество).

Тем не менее криминализация этих деяний шла независимо друг от друга, в результате чего законодательство различных стран, даже в пределах одного географического региона, весьма неоднородно, нормы об уголовной ответственности предусматривают различные криминообразующие признаки

8. Уголовное законодательство Российской Федерации, направленное на борьбу с компьютерными преступлениями, имеет значительное число недостатков и пробелов и требует модернизации существующих норм. С учетом анализа оснований для криминализации деяний, а также требований законодательной техники и правил установления наказуемости деяний, предлагается изложить Главу 28 УК РФ в следующей редакции:

Глава 28. Преступления в сфере компьютерной информации.

Статья 272[1]. Несанкционированный доступ к компьютерной системе

Несанкционированный умышленный доступ к компьютерной системе или ее части, сопровождающийся преодолением установленной на компьютере системы защиты, —

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года.

Статья 272[2]. Неправомерное завладение компьютерной информацией

Несанкционированное копирование или иное неправомерное завладение информацией, хранящейся в компьютерной системе или компьютерной сети, а равно незаконный умышленный перехват компьютерных данных, идущих с одной компьютерной системы на другую, либо данных в пределах одной компьютерной системы, —

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до ста восьмидесяти часов, либо исправительными работами на срок от

шести месяцев до одного года, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок до двух лет.

Статья 272[3]. Модификация компьютерной информации

1. Несанкционированное умышленное изменение компьютерной информации, а равно внесение в нее заведомо ложных данных при отсутствии признаков хищения чужого имущества или незаконного приобретения права на чужое имущество, причинившее значительный ущерб или создавшее угрозу его причинения, —

наказывается штрафом в размере до сорока тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех месяцев, либо обязательными работами на срок от ста до ста восьмидесяти часов, либо исправительными работ на срок до одного года, либо арестом на срок до трех месяцев, либо лишением свободы на срок до двух лет.

2. Несанкционированное умышленное изменение компьютерной информации, а равно внесение в нее заведомо ложных данных при отсутствии признаков хищения чужого имущества или незаконного приобретения права на чужое имущество, если оно совершено с целью скрыть другое преступление или облегчить его совершение, —

наказывается лишением свободы на срок до четырех лет.

Статья 272[4]. Компьютерный саботаж

1. Умышленные ввод, передача, изменение, уничтожение компьютерных данных или компьютерных программ или другое вмешательство в компьютерные системы с целью воспрепятствовать функционированию компьютера или телекоммуникационной системы, —

наказываются штрафом в размере до сорока тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех месяцев, либо обязательными работами на срок от ста до ста восьмидесяти часов, либо исправительными работ на срок до одного года, либо арестом на срок до трех месяцев, либо лишением свободы на срок до двух лет.

2. Те же деяния, если они повлекли по неосторожности тяжкие последствия, —

наказываются лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание вредоносной компьютерной программы или внесение изменений в существующую программу, заведомо приводящих к не-

санкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы компьютера, компьютерной системы или компьютерной сети, а равно использование либо распространение такой программы или машинного носителя с такой программой, –

наказывается штрафом в размере до сорока тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех месяцев, либо обязательными работами на срок от ста до ста восьмидесяти часов, либо исправительными работ на срок до одного года, либо арестом на срок до трех месяцев, либо лишением свободы на срок до двух лет.

2. Те же деяния, если они повлекли по неосторожности тяжкие последствия, –

наказываются лишением свободы на срок до пяти лет.

Статья 274. Исключена.

9. Предлагается дополнить Главу 21 Уголовного кодекса РФ (Преступления против собственности), дополнить следующей статьей:

159^1. Компьютерное хищение

1. Хищение чужого имущества или приобретение права на чужое имущество, совершенное путем ввода, изменения, удаления или блокирования компьютерных данных либо любого другого вмешательства в функционирование компьютера или компьютерной системы, –

наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок от двух до четырех месяцев, либо лишением свободы на срок до двух лет.

2. Компьютерное хищение, совершенное группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину, –

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо исправительными работами на срок от одного года до двух лет, либо лишением свободы на срок до пяти лет.

3. Компьютерное хищение, совершенное лицом с использованием своего служебного положения, а равно в крупном размере, –

наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет либо лишением свободы на срок от двух до шести лет со штрафом в размере до десяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового.

4. Компьютерное хищение, совершенное организованной группой либо в особо крупном размере, –

наказывается лишением свободы на срок от пяти до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового.

Апробация результатов исследования. Основные положения диссертационного исследования выносились на обсуждение на следующих научных конференциях: «III Международная конференция «Информационные технологии и безопасность» (Партенит, Украина, 2003 г.), «Актуальные проблемы государства и права» (Владивосток, 2003 г.), «Новые проблемы юридической науки» (доклад «Криминализация электронных посягательств» на пленарном заседании конференции, Владивосток, 2004 г.).

С 2002 по 2005 гг. автором в качестве исследователя Владивостокского Центра по изучению организованной преступности велась работа по гранту Американского университета (г. Вашингтон) по теме «Киберпреступность и кибертерроризм».

Материалы исследования публиковались на сайтах Владивостокского центра по изучению организованной преступности (http://www crime.vl.ru), Запорожского центра исследования проблем компьютерной преступности (http://www.crime-research.ru).

Основные положения работы отражены в девяти публикациях, посвященных киберпреступности и проблемам борьбы с ней.

Диссертация состоит из введения, трех глав, заключения и списка литературы, использованной при написании диссертационного исследования.

СОДЕРЖАНИЕ РАБОТЫ

Первая глава: «Киберпреступность: понятие, виды, состояние» состоит из трех параграфов.

В первом параграфе «Информационные технологии и преступность. Понятие киберпреступности, киберпреступления и компьютерного преступления» раскрывается проблема взаимосвязи преступности и информационных технологий, дается краткий обзор появления и истории киберпреступности. Автор отмечает, что проявление преступности в сфере компьютерной информации и телекоммуникаций связано с появлением компьютерных сетей и созданием информационной мегасреды. По мере все большего использования компьютерных технологий в различных сферах деятельности, растет и количество преступлений, и размер причиняемого в результате их совершения ущерба. Таким образом, киберпреступность является одним из закономерных негативных последствий развития информационных технологий.

Всестороннее исследование феномена киберпреступности затрудняется тем, что в настоящее время отсутствует общепринятое определение киберпреступности и, кроме того, в силу различий правовых систем, используемых в разных государствах и новизны проблемы делинквентного поведения, понятие «киберпреступность» как юридический термин используется далеко не во всех странах мира.

Очень часто термин «киберпреступность» употребляется в качестве синонима понятия «компьютерная преступность». По мнению автора, эта позиция является неверной. Несмотря на то, что эти термины очень близки друг другу, они все-таки не синонимичны. Понятие «киберпреступность» (в англоязычном варианте — cybercrime) шире, чем «компьютерная преступность» (computer crime), и более точно отражает природу такого явления, как преступность в информационном пространстве. С помощью анализа этимологии слова «киберпреступность» в работе обосновывается необходимость употребления именно этого термина для наиболее точного определения феномена преступности в сфере информационных технологий. Обращается внимание на то, что в работах зарубежных ученых и документах международных организаций также отдается предпочтение термину «киберпреступность», а не «компьютерная преступность».

Употребление понятия «киберпреступность» позволит избежать определенных трудностей при классификации «компьютерных» преступлений. Поскольку термин «компьютерное преступление» перестал охватывать все противоправные деяния в данной сфере, существует точка зрения, что «компьютерные преступления» необходимо

классифицировать на «собственно компьютерные преступления» и «смежные преступления». Таким образом, под «компьютерным преступлением» подразумевается гораздо более широкий спектр деяний, чем это следует из буквального толкования термина. Точка зрения автора заключается в том, что необходимо дать преступлениям такого рода более широкое определение, которое охватит как компьютерные преступления, так и смежные, исключая совпадения названий групп, на которые можно в дальнейшем подразделить данные деяния, с первоначальным термином.

Поскольку киберпреступность – это преступность в информационном, или, иначе говоря, киберпространстве, для того, чтобы дать ей определение, необходимо осмыслить такое понятие, как «киберпространство» В связи с этим в работе уделяется внимание различным трактовкам термина «киберпространство». Тем не менее, по мнению автора, в самом определении «киберпреступность» нет необходимости расшифровывать термин «киберпространство», дабы не перегружать его излишними подробностями и не создавать дефиницию внутри дефиниции. С учетом рекомендаций экспертов ООН, а также документов иных международных организаций, диссертантом сформулировано следующее определение киберпреступности и киберпреступления:

Киберпреступность – это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

Киберпреступление – это виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, а также с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера информационному пространству.

Термин «киберпреступление» охватывает весь спектр преступлений в сфере информационных технологий, будь это преступления, совершенные с помощью компьютеров, или преступления, предметом

которых являются компьютеры, компьютерные сети и хранящаяся на этих носителях информация. Компьютерное преступление – это только то преступление, которое посягает на безопасное функционирование компьютеров и компьютерных сетей, а также на обрабатываемые ими данные. Таким образом, если рассматривать соотношение этих двух понятий, то компьютерное преступление является разновидностью киберпреступления.

Второй параграф «Виды киберпреступлений. Кибертерроризм и информационные войны» посвящен типологии киберпреступлений. Автором рассмотрены достоинства и недостатки существующих классификаций подобного рода преступлений, и на основе этого анализа предлагается выделить следующие виды киберпреступлений:

1) Насильственные или иные потенциально опасные киберпреступления, посягающие на физическую безопасность, жизнь и здоровье человека;

2) Преступления, посягающие на конфиденциальность информации – незаконный доступ к компьютерам или компьютерным системам без причинения ущерба информации.

3) Деструктивные киберпреступления, заключающиеся в повреждении данных и посягающие на целостность данных и безопасность функционирования компьютерных систем. Такие преступления также могут причинить имущественный ущерб, но они не связаны с хищением информации, данных, денежных средств.

4) Преступления, посягающие на имущество, имущественные права, а также на право собственности на информацию и авторские права.

5) Преступления, посягающие на общественную нравственность.

6) Преступления, посягающие на общественную безопасность.

7) Иные киберпреступления, которые условно можно назвать «computer-facilitated» (традиционные преступления, совершение которых компьютер облегчает, или дает новые возможности для их совершения) – преступления, совершаемые посредством компьютерных сетей, и посягающие на различные охраняемые законом объекты. В эту группу входят различные преступления, но их объединяет тот признак, что все они могут быть совершены и без применения компьютерных технологий, информационные технологии в их совершении играют вспомогательную роль.

Каждый из указанных видов киберпреступлений охарактеризован в работе.

Отдельное внимание уделяется таким явлениям, как кибертерроризм и информационные войны. Поднимается проблема не только совершения террористических действий с помощью информационных технологий -- вопрос о такой возможности в настоящее время является дискуссионным, но и использования киберпространства террористическими группами для осуществления и популяризации своей деятельности, а не для непосредственного совершения терактов.

Несмотря на то, что история террористических групп в киберпространстве началась совсем недавно, к 2000 году практически все террористические группы обнаружили свое присутствие в сети Интернет. В 2003 -- 2004 гг. обнаружено сотни сайтов, обслуживающих террористов и их сторонников Автором приводятся следующие основные способы использования глобальных информационных сетей в террористических целях:

1. Сбор с помощью Интернета подробной информации о предполагаемых целях, их местонахождении и характеристике.
2. Сбор денег для поддержки террористических движений.
3. Создание сайтов с подробной информацией о террористических движениях, их целях и задачах, публикация на этих сайтах данных о времени и встрече людей, заинтересованных в поддержке террористов, указаний о формах протеста и т.п., т. е. синергетическое воздействие на деятельность групп, поддерживающих террористов.
4. Вымогательство денег у финансовых институтов с тем, чтобы те могли избежать актов кибертерроризма и не потерять свою репутацию.
5. Использование Интернета для обращения к массовой аудитории для сообщения о будущих и уже спланированных действиях, а также предание террористами с помощью Интернета широкой огласке своей ответственности за совершение террористических актов.
6. Использование Интернета для информационно-психологического воздействия, в том числе инициация «психологического терроризма».
7. Перенесение баз подготовки террористических операций
8. Вовлечение в террористические сети ничего не подозревающих соучастников — например, хакеров, которым неизвестно, к какой конечной цели приведут их действия.
9. Использование возможностей электронной почты или электронных досок объявлений для отправки зашифрованных сообщений для планирования и координации действий.

10. Размещение в Интернете сайтов террористической направленности, содержащих информацию о взрывчатых веществах и взрывных устройствах, ядах, отравляющих газах, а также об их самостоятельном изготовлении.

«Сетевые» и «информационные» войны характеризуются автором как новый способ ведения конфликтов на социальном уровне, без традиционного использования военной силы, с помощью информационных технологий.

В третьем параграфе — «Состояние и тенденции киберпреступности» дается характеристика некоторых криминологических аспектов киберпреступности. Прежде всего, диссертант уделяет внимание проблемам изучения состояния киберпреступности. Это вызвано тем, что для киберпреступности, как ни для какого вида преступности, характерен признак латентности. Поэтому первый этап криминологической характеристики — оценка официальных статистических данных по изучаемому виду преступности — не даст и не может дать реального представления о масштабах киберпреступности. В связи с этим как альтернативные рассматриваются такие методы сбора данных о киберпреступности, как интервьюирование, фокусные группы, обзоры, и способ, условно называемый автором «метод регистрации обращений».

Для иллюстрации состояния и динамики киберпреступности в мировом масштабе в работе использованы и проанализированы как статистика киберпреступности, полученная международными организациями, занимающимися исследованием этой проблемы, так и данные национальных обзоров некоторых государств — США, Великобритании, Австралии Проанализирована также официальная статистика российских и зарубежных правоохранительных органов. И на общемировом уровне, и на уровне отдельных государств киберпреступность характеризуется быстрыми темпами роста и причинением подобного рода преступлениями значительного финансового ущерба гражданам и организациям при минимальном риске для преступника

Так, анализ данных Координационного центра CERT/CC (США), публиковавшего с 1988 по 2003 годы статистику о поступивших жалобах от жертв компьютерных преступлений, показывает, что за 15 лет количество обращений увеличилось почти в 23000 раз.

Центр приема сообщений об Интернет-преступлениях (IC3), существующий при Центре по изучению беловоротничковой преступности ФБР и принимающий жалобы потерпевших из любых стран, с 1 января по 31 декабря 2004 года только через Web-сайт получил 207449 жалоб Это на 66,6% больше, чем в 2003 году, и почти втрое больше, чем в 2002. В течение того же периода 190143 жалобы о мошенничестве были переданы в соответствующие правоохранительные органы (в 2003 году – 95064, в 2002 – 48252 жалобы). Общая сумма ущерба, причиненного преступлениями, жалобы о которых после дополнительной проверки были переданы в правоохранительные органы, в 2004 году составила 68,14 млн. долларов США. Самые высокие денежные потери в 2004 году понесли потерпевшие от мошенничества с чеками – в среднем 3600 $, «нигерийских писем» 3000 $, злоупотребления доверием – 1000 $.

Специалисты одного из ведущих производителей антивирусного программного обеспечения – компании Trend Micro Enterprise подсчитали, что в 2003 году компьютерные вирусы причинили мировому бизнесу ущерб в размере 55 миллиардов долларов В 2002 году, по данным Trend Micro, вирусы нанесли ущерб на сумму от 20 до 30 миллиардов долларов, а в 2001 – 13 миллиардов. Таким образом, ежегодно сумма ущерба удваивается. По данным британской группы Mi2g Intelligence Unit, ущерб от вирусов в 2004 году составил от $166 до $202 млрд. С учетом того, что в мире насчитывается около 600 млн. компьютеров, на один ПК ущерб, в среднем, составит $277–$336. Mi2g Intelligence Unit также сообщает, что в течение 2004 года было заражено около 115 млн. ПК в 200 странах мира.

Исследуется также растущая взаимосвязь киберпреступности и организованной преступности, вызывающая все большее беспокойство специалистов Рассматриваются способы использования глобальных сетей организованными преступными группами, а именно: использование сети Интернет для совершения «традиционных» преступлений (например, вымогательств), отмывания денег, а также в качестве безопасного средства коммуникации.

В качестве факторов, детерминирующих киберпреступность, автором называются и характеризуются политические, экономические, правовые, идеологические и нравственно-психологические факторы, недостатки социального контроля и самодетерминация киберпреступности.

Вторая глава диссертационного исследования «Уголовно-правовые меры борьбы с киберпреступностью на международном уровне и за рубежом» посвящена анализу международно-правового законодательства, а также национального уголовного законодательства зарубежных стран в сфере борьбы с киберпреступностью. Данная глава состоит из двух параграфов.

В первом параграфе — «История международного сотрудничества в борьбе с киберпреступностью» кратко охарактеризованы наиболее значительные документы международных организаций в области борьбы с киберпреступностью — с начала 1980-х г.г. до момента принятия Конвенции Совета ЕС о киберпреступности. Рассматриваются документы ООН, Большой Восьмерки, Организации экономического сотрудничества и развития, Совета Европы - в частности, рекомендация № 89, утвержденная комитетом Министров ЕС 13.09.1989 года и содержащая список правонарушений, рекомендованный странам — участницам ЕС для разработки единой уголовной стратегии, связанной с компьютерными преступлениями. Затем как одно из основных международных соглашений в этой области анализируется Конвенция Совета Европы о киберпреступности. Отмечается, что этот документ, несмотря на очевидную его значимость, не лишен недостатков, которые обусловили отрицательное восприятие Конвенции многими членами сетевого информационного сообщества. Автором рассмотрены положения этого документа, вызвавшие негативную реакцию на принятие Конвенции многими известными специалистами.

Далее в работе уделяется внимание проблемам международного сотрудничества государств, а именно — вопросам криминализации общественно опасных деяний в киберпространстве. Поскольку киберпреступность является трансграничной проблемой, вопрос криминализации общественно опасных деяний в киберпространстве является одним из наиболее важных для осуществления международного сотрудничества Диссертантом рассматриваются проблемы и возможности достижения консенсуса по вопросам криминализации различных видов названных деяний в зависимости от того, на какой объект они посягают.

Второй параграф — «Национальное законодательство стран мира о киберпреступлениях» посвящен сравнительному анализу норм уголовного законодательства зарубежных государств в области борьбы с киберпреступностью. В нем, прежде всего, исследуется взаимо

связь реформирования национального уголовного законодательства зарубежных стран с историей киберпреступности, а также с принятием международных документов, направленных на борьбу с этим явлением. Эта взаимосвязь обусловлена тем, что все большее распространение компьютеров, проникновение их в новые сферы на различных этапах создавало новые общественно опасные посягательства, на которые законодатель должен был реагировать. Диссертантом проанализирована точка зрения зарубежных ученых о том, что эти изменения происходили «волнообразно», и охарактеризованы основные «волны» реформ и их взаимосвязь с развитием киберпреступности.

Автором рассматриваются и сравниваются следующие положения уголовного законодательства зарубежных государств:

- нормы об охране конфиденциальности данных,
- нормы об ответственности за неуполномоченное проникновение в компьютеры и компьютерные сети,
- нормы о защите коммерческой тайны,
- нормы о защите компьютеров и сетей от саботажа,
- нормы об экономических киберпреступлениях (в частности, компьютерном мошенничестве).

Проведение сравнительного анализа законодательства в зависимости от объекта посягательства позволило выявить способы закрепления в уголовных законах норм об ответственности за киберпреступления.

Сравнительный анализ показывает, что законодательство различных стран, даже в пределах одного географического региона, весьма неоднородно, нормы об уголовной ответственности предусматривают различные криминообразующие признаки. Нормы о киберпреступности могут быть как выделены в отдельные статьи УК, так и быть объединены с положениями об ответственности за иные преступления, посягающие на тот же объект. При рассмотрении и сравнении соответствующих норм автором отмечены наиболее удачные, с точки зрения законодательной техники, варианты установления уголовно-правового запрета.

Третья глава — «Законодательство Российской Федерации о киберпреступности: пути совершенствования» состоит из двух параграфов.

В первом параграфе — «Анализ проблем действующего законодательства о преступлениях в сфере компьютерной информации и

возможных путей их решения» — исследуются нормы Главы 28 Уголовного кодекса РФ. Автор обращает внимание на определенные недостатки действующих норм о компьютерных преступлениях и предлагает возможные пути их решения.

Прежде всего, диссертантом предложено заменить термином «компьютер» устаревший термин «ЭВМ», поскольку компьютер и ЭВМ — в современном понимании слова — не одно и то же, ведь компьютер может в принципе быть реализован на иных, неэлектронных технологиях — оптико-волоконных, лазерных, биотехнологиях.

Также предлагается отказаться от употребления понятия «охраняемой законом компьютерной информации», которое фактически выводит из-под уголовно-правовой охраны значительный массив компьютерной информации. В Уголовных кодексах многих государств, а также в Конвенции Совета Европы о киберпреступности преступлением признается незаконный доступ к компьютерным системам или их части. Это позволяет избежать бланкетных норм, противоречий в толковании Уголовного кодекса и законов, к которым он отсылает. При этом, с учетом того, что владелец информации обязан обеспечить ее охрану, может быть криминализован доступ к компьютерной системе или ее части, если он совершен с преодолением систем защиты.

Также отмечается, что само понятие неправомерного доступа является оценочным. Неправомерность может означать как несоответствие нормам права, так и совершение действия при отсутствии прав на его совершение. Эта проблема может быть решена путем замены понятия «неправомерный доступ» термином «несанкционированный доступ».

УК РФ не предусматривает наказания за несанкционированный доступ к информации, не повлекший последствий, указанных в ст. 272. А между тем чтение информации не менее опасно, чем ее копирование. В некоторых случаях достаточно увидеть и прочитать информацию, и она теряет свою ценность или может быть применена в дальнейшем безо всякого копирования. По мнению автора, для нормального функционирования компьютерных систем и обеспечения безопасности хранения и передачи информации, уголовный закон должен защищать компьютер любого пользователя, пользующегося средствами защиты.

В диспозиции статьи 273 УК РФ при описании объективной стороны преступления допущена синонимия единственного и множе-

ственного числа, недопустимая с точки зрения законодательной техники и явно искажающая волю законодателя.

Что же касается статьи 274 УК РФ, то диссертант согласен с мнением ученых (Н.А. Лопашенко), считающих, что данная статья представляет собой пример необоснованной криминализации. В ней говорится о нарушении «правил эксплуатации ЭВМ, системы ЭВМ или их сети», но поскольку в настоящее время не существует нормативно закрепленных правил эксплуатации ЭВМ, то непонятно, нарушение каких правил попадает под указанное деяние. Использование законодателем двух уровней последствий в качестве обязательных признаков состава подчеркивает то, что опасность самого деяния – не велика.

В УК РФ отсутствуют нормы о так называемом «компьютерном мошенничестве», в результате чего подобные деяния в России квалифицируются по совокупности двух статей – ст. 159 и ст. 272 УК РФ. Однако согласно Постановлению Пленума Верховного суда СССР от 5 09.1986 г. № 11 «По делам о хищении личной собственности», признаком мошенничества является добровольная передача потерпевшим имущества или права на имущество виновному под влиянием обмана или злоупотребления доверием. В случае с «компьютерным мошенничеством» потерпевший может ничего не знать о передаче имущества или права на имущество в момент этой передачи, и вообще не желать ее, то есть отсутствует обязательный волевой признак – добровольность. В то же время это деяние не может быть квалифицировано и как кража, поскольку в компьютерах и компьютерных сетях хранятся не деньги или имущество, а информация о них или об их движении.

Предложения о дополнении статьи 159 квалифицирующим признаком, а также расширении ее диспозиции путем указания признака совершения деяния «в том числе с использованием компьютерных технологий», не решают проблемы квалификации по указанным выше причинам. Невозможно также согласиться с предложениями о введении статьи с названием «Компьютерное мошенничество», поскольку понятие мошенничества, использующееся в УК РФ, содержит обязательный волевой признак (добровольная передача имущества), а по правилам законодательной техники термин мошенничество может иметь только одно значение. С учетом изложенного, автор предлагает дополнить УК РФ нормой о «компьютерном хищении».

Во втором параграфе — «Предложения по совершенствованию российского законодательства о киберпреступности» – автором на основе произведенного ранее анализа недостатков существующих норм об ответственности за компьютерные преступления и возможных путей их совершенствования предлагается новая редакция Главы 28 УК РФ.

Указанную главу предлагается пересмотреть путем изменения диспозиции статьи 274 (Несанкционированный умышленный доступ к компьютерной системе или ее части, сопровождающийся преодолением системы защиты), включения новых статей (фактически выделения их из существующей статьи 274), предусматривающих уголовную ответственность за: 1) неправомерное завладение компьютерной информацией; 2) модификацию компьютерной информации; 3) компьютерный саботаж. Кроме того, предлагается исключить статью 274 — «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» и ввести в Уголовный кодекс РФ новую статью - 159.1 — об ответственности за компьютерное хищение.

Поскольку две нормы из предложенных представляют собой предложения по установлению уголовно-правового запрета, в работе проанализированы основания для принятия решения о криминализации этих деяний и обоснована позиция автора о ее необходимости.

При конструировании санкций предлагаемых статей были учтены рекомендации российских ученых по установлению наказуемости деяний. В частности, это рекомендации по обеспечению связи санкций статей, устанавливающих ответственность за покушение на однородные объекты, а также статей, устанавливающих ответственность за разные по степени тяжести преступления по принципу: за равные по степени тяжести преступления должны предусматриваться приблизительно равные наказания. При определении степени общественной опасности преступления — а именно из этого должен исходить законодатель при построении санкций — автором приняты во внимание носящие рекомендательный характер положения Модельного Уголовного кодекса государств — участников СНГ по определению тяжести компьютерных преступлений.

Диссертантом также затронута проблема отсутствия в российском законодательстве норм об ответственности за несанкционированные рассылки — так называемый «спам». Проанализированы последние предложения о введении уголовной ответственности за это деяние,

обосновывается позиция автора, заключающаяся в том, что в настоящее время нет необходимости воздействия на такое явление, как спам, уголовно-правовыми мерами.

В Заключении излагаются выводы и формулируются предложения по совершенствованию уголовного законодательства.

Основные положения работы отражены в следующих публикациях:

1. Тропина Т.Л. Интернет и терроризм: прежние цели – новые средства // Современные проблемы государства и права. Сборник мат. конф. – Владивосток, 2003 – С. 324–327. – 0,16 п.л.

2. Тропина Т.Л. Киберпреступность и кибертерроризм // Организованная преступность, терроризм и коррупция. Криминологический ежеквартальный альманах. № 2. – М., 2003. – С. 140–144. – 0,4 п.л.

3. Тропина Т.Л. Киберпреступность и кибертерроризм: договоримся о понятиях // Проблемы преступности: традиционные и нетрадиционные подходы. – М : Рос. криминол. ассоц, 2003. – С. 14–21. – 0,4 п.л.

4. Тропина Т Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Информаційні технології та безпека – Киев, 2003. – С. 168–175. – 0,4 п.л.

5. Номоконов В.А., Тропина Т.Л. Терроризм с помощью Интернета // Терроризм в России и проблемы системного реагирования. – М.: Рос. криминол. ассоц, 2004. – С. 55–59. 0,24 п.л.

6 Тропина Т.Л. Перевод статьи Д. Льюиса «Оценка риска кибертерроризма, кибервойн и других киберугроз» // Терроризм в России и проблемы системного реагирования. – М.: Рос криминол. ассоц., 2004. – С. 64–80. 0,96 п.л.

7. Тропина Т Л. Киберпреступность и кибертерроризм // Компьютерная преступность и кибертерроризм. Исследования, аналитика Вып. 1. – Запорожье, 2004. – С. 76–82. – 0,4 п.л.

8. Тропина Т.Л. Криминализация киберпреступлений: достижение консенсуса // Компьютерная преступность и кибертерроризм. Исследования, аналитика. Вып 2. – Запорожье, 2004. – С. 49–56. – 0,5 п.л.

9. Тропина Т.Л. Криминализация электронных посягательств // Новые проблемы юридической науки. – Сборник мат. конф. Владивосток, 2005. – С 264–271 – 0,36 п.л.

Тропина Татьяна Львовна

КИБЕРПРЕСТУПНОСТЬ: ПОНЯТИЕ, СОСТОЯНИЕ, УГОЛОВНО-ПРАВОВЫЕ МЕРЫ БОРЬБЫ

АВТОРЕФЕРАТ

Подписано в печать 23.08. 2005 г.
Формат 60x84 1/16. Усл. печ. л. 1,5. Уч. изд. л. 1,68.
Тираж 120 экз. Заказ 108

Издательство Дальневосточного университета
690950, г. Владивосток, ул. Октябрьская, 27

Отпечатано в типографии
Издательско-полиграфического комплекса ДВГУ
690950, г. Владивосток, ул. Алеутская, 56