ГАСАНОВ Р.Т., аспирант
(Национальная Академия наук Азербайджана)

УДК 343.3/.7 : 341.4

БОРЬБА С КИБЕРПРЕСТУПНОСТЬЮ В РАМКАХ СОВЕТА ЕВРОПЫ И ЗАКОНОДАТЕЛЬСТВА АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ

Розглянуто питання боротьби з кіберзлочинністю в рамках Ради Європи й законодавства Азербайджанської Республіки. Досліджено конвенції й рішення (зокрема, Конвенції Ради Європи про протидію кіберзлочинності) Ради Європи по боротьбі з кіберзлочинністю.

Ключові слова: *законодавство, кіберзлочинність, інтернет- злочинність, кібертероризм.*

Рассмотрены вопросы борьбы с киберпреступностью в рамках Совета Европы и законодательства Азербайджанской Республики. Исследованы конвенции и решения (в частности, Конвенции Совета Европы о противодействии киберпреступности) Совета Европы по борьбе с киберпреступностью.

Ключевые слова: *законодательство, киберпреступность, интернет- преступность, кибертерроризм.*

This article is devoted to the issues of fight against cybercrime in the Council of Europe and legislation of Republic of Azerbaijan. Author has been investigated convention and decisions (especially the Convention on Cybercrime of the Council of Europe) of the Council of Europe on fight against cybercrime.

Keywords: *Legislation, cybercrime, internet crime, cyber-terrorism.*

В 1960-х годах, когда появились первые транзисторные вычислительные системы и популярность компьютеров начала расти, уголовно наказуемым признавалось главным образом физическое повреждение компьютерных систем и хранящихся на них данных. В 1970-х годах произошел переход от традиционных имущественных преступлений против компьютерных систем к новым формам преступности, в частности, противоправному использованию компьютерных систем и манипуляциям с электронными данными. В 1980-х годах популярность персональных компьютеров продолжала расти и впервые в истории управление многими важнейшими объектами инфраструктуры стало осуществляться при помощи компьютерных технологий [1, с. 217].

Одним из побочных эффектов распространения компьютерных систем стало повышение интереса к программному обеспечению и появление первых форм торговли "пиратскими" программными продуктами и преступлений, связанных с патентами. Кроме того, появление компьютерных сетей позволило преступникам получать доступ к тем или иным компьютерным системам, не присутствуя при этом на месте преступления [2, с.428].

Появление в 1990-е гг. графического интерфейса (Всемирная сеть World Wide Web) и последовавший за этим стремительный рост числа пользователей Интернета привели к возникновению новых методов совершения преступных деяний. Так, например, если детские порнографические материалы распространялись путем физического обмена печатной продукцией и видеозаписями, то теперь такие материалы распространяются через веб-сайты и Интернет-службы [3, с. 9].

Компьютерные преступления, как правило, совершались на местном уровне, однако с появлением Интернета электронная преступность приобрела транснациональный характер. В первом десятилетии XXI века на передний план вышли новые, более изощренные методы совершения преступлений, такие как "фишинг"13, "атаки с использованием бот-сетей", а также новые методы использования технологий, в частности, речевая связь по Интернету (IP-телефония) (VoIP) и "облачные вычисления" ("cloud computing"), которые затрудняют деятельность правоохранительных органов.

Сами хакеры говорят, что успех взлома зависит от интеллектуальных способностей. Все это свидетельствует об *интеллектуальном характере Интернет-преступности.* Интеллектуальность среди компьютерных преступников пропагандируется также посредством субкульту-

ры хакеров, что дает стимул Интернет-преступнику для умственного саморазвития. Есть и другие виды преступлений, которые требуют определенных профессиональных знаний и интеллектуальных способностей, например, беловоротничковая преступность [4, с. 343-347].

Среди признаков Интернет-преступности можно выделить ее *транснациональный характер.* По мнению некоторых авторов, около 62 % компьютерных преступлений совершается в составе организованных групп, в том числе находящихся на территории нескольких стран. Например, преступные группировки, занимающиеся рекламой и распространением детской порнографии через Интернет, зачастую состоят из жителей различных стран СНГ и зарубежья. При этом соблюдается полная анонимность, взаимодействие происходит посредством Глобальной компьютерной сети через пароли и клички. Как правило, в лицо никто из участников друг друга не знает. Посредством Интернета можно осуществлять многие трансграничные операции, особенно касающиеся передачи данных, чем и пользуются преступники [5, с. 74].

Законодательное регулирование киберпространства в одной отдельно взятой стране вряд ли возможно. Однако без государственного контроля компьютерных сетей обойтись нельзя, хотя бы потому, что глобальные компьютерные сети, подобные Internet, как и всякая чрезвычайно эффективная технология, могут быть использованы не только во благо. Очевидно, что данное противоречие можно устранить только в рамках международного права. В силу этого тенденция к расширению международного сотрудничества в борьбе с преступностью в сфере высоких технологий отмечается в деятельности многих международных организаций. Одной из них является Совет Европы (СЕ), по мнению которого рост компьютерной преступности требует согласованного подхода государств к выработке предписаний, направленных на борьбу с ней. Этой проблеме посвящен ряд принятых СЕ рекомендаций, в которых сделана попытка определить понятие и очертить круг "преступлений, связанных с использованием компьютерных технологий". Однако рекомендательный характер этих документов не способствует разрешению возникающих на практике коллизий, для чего необходимы полноценные международно-правовые документы.

Осознание этого повлекло за собой формирование Комитетом министров СЕ в феврале 1997 г. Комитета экспертов по преступности в киберпространстве, перед которым была поставлена задача изучить юридические проблемы, возникающие при расследовании компьютерных преступлений. По результатам изучения им был разработан проект Конвенции о киберпреступности. Реакция правозащитных организаций на проект Конвенции оказалась вполне ожидаемой. В открытом письме правозащитных групп к СЕ утверждается, что проект "противоречит известным нормам защиты личности, неоправданно усиливает полномочия национальных правительств, подрывает развитие методов обеспечения безопасности информации, что уменьшает ответственность государств перед законом". После открытого обсуждения проект доработан с учетом требований усиления гарантий неприкосновенности частной жизни и подготовлен к обсуждению исполнительными органами СЕ. В период с 18 по 22 июня 2001 г. проект обсужден на заседании Европейского комитета по проблемам преступности, которым в него внесены некоторые изменения и принято решение о вынесении проекта Конвенции для принятия и подписания Комитету Министров СЕ [6, с.2].

Сегодня Азербайджан не испытывает проблем со специалистами информационной безопасности. В вузах страны действуют соответствующие факультеты. Кроме того, специалистов в этой области уже два года готовят и в Академии национальной безопасности имени Гейдара Алиева. Также необходимо напомнить, что киберпреступность в результате внесенных в 2000 г. в Уголовный кодекс АР изменений была признана уголовно наказуемым видом преступления. Между тем, по мнению экспертов, законодательство Азербайджана в данной сфере требует корректировки в соответствии с требованиями Конвенции Совета Европы по борьбе с киберпреступностью. В прошлом году Азербайджан подключился к Конвенции по киберпреступности, принятой Советом Европы в 2001 году. Преступления, совершенные посредством всемирной сети на территории страны, караются согласно статьям 271-273 Уголовного кодекса Азербайджана:

- *неправомерный доступ к компьютерной информации*. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе электронно-вычислительных машин или

их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети (статья 271);

- *создание, использование и распространение вредоносных программ для ЭВМ*. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами (статья 272);

- *нарушение правил эксплуатации электронно-вычислительных машин (ЭВМ), системы ЭВМ или их сети.* Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред (статья 273).

Известно, что транснациональные организованные преступные группы широко используют современные информационно-коммуникационные технологии. Международные террористические организации стремятся использовать научно-технические достижения и привлечь в свои ряды специалистов в области связи, компьютерных, информационно-коммуникационных технологий и т.д. Эти террористические организации активно пользуются Интернетом для постоянного набора новых членов, оправдания совершенных терактов, подготовки потенциальных террористов, поддержания связи между членами групп и других целей. В последнее время киберпреступления, в особенности кибертерроризм, принимают все более опасный характер, что увеличивает необходимость совершенствования деятельности Министерства национальной безопасности по предотвращению этих преступлений. Борьба с незаконными действиями в этой области требует соответствующего технического оборудования, а также специальных знаний и навыков в сфере высоких технологий. В последние годы было уделено большое внимание именно указанным сферам, приняты адекватные меры по усовершенствованию возможностей по борьбе с киберугрозами для нашей страны.

Конвенция о киберпреступности представляет собой комплексный документ, содержащий нормы, призванные оказать существенное влияние на различные отрасли права: уголовное, уголовно-процессуальное, авторское, гражданское, информационное. Она базируется на основных принципах международного права: уважения прав человека, сотрудничества и добросовестного выполнения обязательств. Нормы Конвенции направлены на регулирование трех основных блоков вопросов:

- сближение уголовно-правовой оценки преступлений в сфере компьютерной информации;
- сближение национальных уголовно-процессуальных мер, направленных на обеспечение собирания доказательств при расследовании таких преступлений;
- международное сотрудничество в уголовно-процессуальной деятельности, направленной на собирание доказательств совершения таких преступлений за рубежом.

Уголовно-правовые вопросы

Конвенцией предлагается включить в законодательство стран-участниц единые нормы уголовной ответственности за “киберпреступления”, перечень которых включает (1) деяния, направленные против компьютерной информации (как предмета преступного посягательства), и использование ее в качестве уникального орудия совершения преступления, и (2) деяния, предметом посягательства которых являются иные охраняемые законом блага, а информация, компьютеры и т.д. являются лишь одним из элементов объективной стороны преступления в качестве, к примеру, орудия его совершения, составной части способа совершения или сокрытия.

Уголовно-процессуальные аспекты

Одной из главных особенностей Конвенции является предложение исходить из того положения, что главенствующая роль в регулировании уголовного процесса расследования преступлений в сфере компьютерной преступности принадлежит национальному законодательству. В силу этого Конвенция включает главу “Меры, которые надлежит принять на национальном уровне”, в которой предусмотрено включение в национальный уголовный процесс норм, регламентирующих процессуальные действия, специфические для расследования и

судебного разбирательства по делам о компьютерных преступлениях (ст. 14-23).

В круг процессуальных норм, предлагаемых Конвенцией для включения в национальное законодательство, входят прежде всего известные следственные действия, дополненные рядом особенностей, связанных со спецификой, присущей доказательственной информации в форме компьютерных данных. В силу этого круг процессуальных институтов предлагается дополнить новым видом обыска и выемки. ст. 19 "Обыск и выемка хранимых компьютерных данных" Конвенции содержит предписания о том, что:

- обыску или иному подобному следственному действию, обеспечивающему непосредственное получение доказательственной информации, могут быть подвергнуты (a) компьютерные системы или их части, а также хранящиеся там компьютерные данные, и (b) среда для хранения компьютерных данных, в которой могут храниться искомые компьютерные данные;

- если в ходе обыска имеются основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части и когда такие данные доступны из первой системы или могут быть получены с ее помощью, компетентные органы должны быть вправе незамедлительно "распространить" производимый обыск на эту другую систему;

- при обнаружении искомых компьютерных данных компетентные органы должны быть вправе:

a) произвести выемку вычислительной системы, ее части или среды для хранения компьютерных данных либо иным подобным образом наложить арест на них;

b) изготовить и сохранить копии соответствующих компьютерных данных;

c) обеспечить сохранение целостности относящихся к делу хранимых компьютерных данных;

d) сделать эти компьютерные данные в компьютерной системе, доступ в которую был получен, недоступными или удалить их из нее.

- для обеспечения выемки требуемых компьютерных данных компетентные органы вправе обязать любое лицо, обладающее знаниями о функционировании соответствующей компьютерной системы или применяемых мерах защиты, оказать соответствующую помощь.

Наряду с этим Конвенция предусматривает необходимость формирования на внутригосударственном уровне правовых основ новых процессуальных действий. К ним отнесены, во-первых, *незамедлительное обеспечение сохранности хранимых компьютерных данных, включая данные о потоках информации*, которые были генерированы и сохранены с помощью компьютерной системы, когда имеются основания полагать, что эти данные особенно подвержены риску потери или модификации (ст. 16). Оно должно осуществляться на основе распоряжения компетентных органов, отданного любому лицу, во владении или под контролем которого находятся компьютерные данные. Конкретный срок сохранения не установлен, но обозначен как "адекватный период времени, который позволит компетентным органам добиться раскрытия этих компьютерных данных". Это означает, что предлагаемый процессуальный институт не дает правовых оснований для прямого доступа органов власти к компьютерной информации, а лишь создает условия для него, являясь мерой предварительного характера. При этом под сохранностью данных следует понимать оставление их в том виде, в каком они уже имеются в ЭВМ, защитив от любых внешних воздействий.

Во-вторых, *незамедлительное обеспечение сохранности и частичное раскрытие данных о потоках информации* (ст. 17). Оно отличается от предыдущего тем, что подлежит применению в случаях, когда речь идет о необходимости сохранения сведений о сообщениях электросвязи, передаваемых по компьютерным сетям. Это должно позволить незамедлительно сохранять данные о потоках информации "независимо от того, один или большее число поставщиков услуг были вовлечены в передачу соответствующего сообщения", а с другой – незамедлительно раскрывать эти данные компетентным органам в объемах, достаточных, чтобы "идентифицировать поставщиков услуг и путь, которым передавалось сообщение", то есть фактически для того, чтобы оперативно отследить прохождение компьютерной информации в сетях от точки ввода до конечного адресата.

В-третьих, *отдача распоряжения о предъявлении* (ст. 18). Такое распоряжение может быть отдано (1) лицу – о предъявлении компьютерных данных, находящихся под контролем этого лица, хранящихся в компьютерной системе или в иной среде для хранения компьютерных данных, (2) поставщику услуг – сведений о его абонентах. К последним отнесена любая имеющаяся у поставщика услуг информация о пользователях, выраженная как в форме компь-

ютерных данных, так и в любой другой форме (за исключением данных о потоках или содержании информации), с помощью которой можно установить: тип использованной связи, ее технические условия и время осуществления; личность пользователя, его адрес, номера телефонов и иных средств доступа, сведения о выставленных ему счетах и произведенных им платежах; любые другие сведения о месте установки коммуникационного оборудования. Следует отметить, что Конвенция допускает применение данного вида новых полномочий строго на индивидуальной основе для решения задач расследования конкретных уголовных дел. В связи с этим нужно понимать, что эти полномочия не должны использоваться для того, чтобы заставить всех поставщиков услуг постоянно накапливать и хранить сведения о своих абонентах, всю передаваемую ими компьютерную информацию и т.д.

В-четвертых, *сбор и запись с применением технических средств в режиме реального масштаба времени данных о потоках информации, передаваемых через компьютерные системы* (ст. 20). Конвенцией предусмотрено наделение полномочиями осуществлять эту деятельность как компетентных органов государства, так и по их указанию поставщиков услуг. Данный вид деятельности рассчитан на применение в отношении сведений о сообщениях, передаваемых по сетям электросвязи, которые формируются (создаются) непосредственно в момент реализации таких полномочий. При этом осуществляется передача нематериальных объектов (например, в форме электромагнитных импульсов), а их сбор и запись не мешают прохождению самого сообщения по сетям электросвязи до адресата.

В-пятых, перехват (собирание и запись) данных о содержании сообщений, передаваемых с помощью компьютерных систем (ст. 21), осуществляемый как компетентными органами государства, так и поставщиками услуг по их указанию. Данный институт аналогичен предыдущему, но касается непосредственно содержательной части сообщений, передаваемых по сетям электросвязи.

Вопросы международного сотрудничества

Подробное изложение в Конвенции норм, подлежащих включению в национальное уголовно-процессуальное законодательство, создало необходимые условия для определения в ней основных принципов международного сотрудничества ее участников, к которым ст. 23 отнесены:

- максимально широкие пределы сотрудничества, правовой основой которого должны являться международные документы, согласованные договоренности на основе единообразного и взаимодополняющего законодательства, а также нормы внутригосударственного права;
- осуществление сотрудничества при расследованиях или судебном преследовании в отношении уголовных преступлений, связанных с любыми компьютерными системами и компьютерными данными.

В целом вопросам сотрудничества компетентных органов различных государств в борьбе с компьютерными преступлениями посвящена гл. 3 Конвенции «Международное сотрудничество». В ее содержании следует выделить несколько ключевых аспектов.

Порядок сношений

При расследовании преступлений в сфере компьютерной информации большинство запросов о взаимной правовой помощи касаются вопросов, так или иначе затрагивающих конституционные права граждан. В силу этого Конвенция исходит из того, что принятие решений по данным ходатайствам должно находиться в исключительной компетенции одного-двух центральных органов, вне зависимости от подследственности и подведомственности конкретных уголовных дел (с учетом лишь специфики стадий следствия – предварительного и судебного). Именно специально назначенные центральные органы должны поддерживать связь непосредственно друг с другом. С учетом специфики расследования таких преступлений Конвенцией предусмотрено дополнение общего порядка сношений при оказании взаимной правовой помощи. Так, в соответствии с ч. 3 ст. 25 в обстоятельствах, не терпящих отлагательства, допускается направление запросов о взаимной правовой помощи или сообщений, связанных с такими запросами, с использованием оперативных средств связи, включая факсимильные сообщения или электронную почту, если такие средства обеспечивают соответствующие уровни безопасности и подтверждения подлинности, с последующим официальным подтверждением по требованию запрашиваемой стороны. Согласно пунктам «a» и «b» части 9 ст. 27 Конвенции запросы о взаимной правовой помощи или связанные с ними сообщения могут направляться непосредственно

судебными органами сторон, а также через МОУП (Интерпол) [7, с. 17-25].

Но правоохранительные органы – лишь часть решения. Необходимо также, чтобы отдельные пользователи и компании понимали, в чем состоит опасность, и имели достаточные знания и инструментарий, чтобы свести к минимуму риск стать жертвой киберпреступников. Это особенно важно для пользователей, которые зачастую несведущи в технике и плохо понимают, какие потенциальные проблемы таят в себе онлайн-покупки, интернет-банкинг и социальные сети. Проблему усугубляет также растущее число пользователей, соединяющихся с Интернетом впервые. Необходимо выработать разнообразные творческие подходы для повышения уровня понимания обществом проблем, связанных с киберпреступностью, и методов, позволяющих уменьшить риск до минимума.

Список использованной литературы:

1. McLaughlin, Computer Crime: The Ribicoff Amendment to United States Code, Title 18 // Criminal Justice Journal. – 1978. – Vol. 2. – P. 217 et seq.

2. BloomBecker, The Trial of Computer Crime // Jurimetrics Journal. Vol. -21. – 1981. – P. 428.

3. Child Pornography, CSEC World Congress Yokohama Conference, 2001, p. 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, United States House of Representatives, 109th Congress, 2007, p. 9.

4. Криминология / Под. ред. Дж. Ф. Шели; Пер. с англ. – СПб., 2003. – С. 343-347.

5. Кашапов Р.М., Наумов С.С. Проблемы с распространением детской порнографии в глобальной сети Интернет // Вестник Дальневосточного юридического института МВД России. – 2004. – № 2. – С. 74.

6. Draft Convention on Cyber-crime and Explanatory memorandum related thereto: final activity report. Prepared by Committee of Experts on Crime in Cyber-Space (PC-CY) Submitted to European Committee on Crime Problems (CDPC) at its 50 th plenary session (18-22 June 2001). – Secretariat Memorandym prepared by the Directorate General of Legal Affairs. Restricted, CDPC (2001) 2 rev 2. – Strasbourg, 20 June 2001. .

7. Волеводз А.Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 17-25.

Надійшла до редакції 04.07.2011

МИРЗОЕВ Р.А., аспирант
(Бакинский государственный университет)

УДК 347.21

СУТЬ И СОДЕРЖАНИЕ ЗАЩИТЫ ИМУЩЕСТВЕННЫХ ПРАВ ИНОСТРАННЫХ ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ

Суть і зміст захисту майнових прав іноземних фізичних і юридичних осіб проаналізовано на основі розбіжностей у правовій літературі й міжнародній практиці. Зазначено, що перехід захисту майнових прав іноземних осіб у сферу міжнародно-правового регулювання визначає необхідність розв'язання низки питань, що перебувають у центрі уваги дослідження. Зроблено висновок про те, що право захисту майнових прав іноземних осіб поєднує в собі матеріально-правові й процесуально-правові сторони.

Ключові слова: *майнові права, захист, охорона, реалізація прав, міжнародне право, судова юрисдикція, дипломатичний захист, конвенція.*

Суть и содержание защиты имущественных прав иностранных физических и юридических лиц проанализированы на основе разногласий в правовой литературе и международной практике. Отмечено, что переход защиты имущественных прав иностранных лиц в сферу международно-правового регулирования предопределяет необходимость решения ряда вопросов, находящихся в центре внимания исследования. Сделан вывод о том, что право защиты имущественных прав иностранных лиц объединяет в себе материально-правовые и процессуально-правовые стороны.

Ключевые слова: *имущественные права, защита, охрана, реализация прав, международное право, судебная юрисдикция, дипломатическая защита, конвенция.*

In article the essence and the maintenance of protection of property rights of foreign physical and juridical bodies are analyzed on the basis of disagreements in the legal literature and