Джансараева Р.Е., Аратулы К.

Международное сотрудничество в борьбе с киберпреступностью

В мировой правовой литературе выделяют четыре вида компьютерных преступлений, связанных с нарушением конфиденциальности, целостности и доступности компьютерных данных и сети. Остальные преступления, в которых компьютер является орудием или средством совершения преступлений, должны рассматриваться как традиционные преступления, но правовые механизмы их расследования должны быть адекватными средствами совершения этих преступлений.

Ключевые слова: киберпреступность, международное сотрудничество, киберпреступник, ООН, борьба с преступностью, международные соглашения.

Jansarayeva R.E., Aratuly K.

International cooperation in the fight against cybercrime

In world law literature allocate four classes of computer crimes. They relate to the violation of confidentiality, integrity and availability of computer information and computer system or network. Other crimes in which computer is tool or means commit crimes should be view as tradition crimes. But, the legal mechanism their investigation should be adequate means commit these crimes.

Key words: cybercrimes, international cooperation, UN, combating crimes, cybercriminal, international agreements.

Жансараева Р.Е., Аратұлы Қ.

Киберқылмыстылықпен күресудегі халықаралық байланыс

Әлемдік құқықтық әдебиеттерде ақпараттық қылмыстардың негізгі төрт түрін ерекшелеп көрсетеді. Олар құпиялықты, компьютерлік мәліметтердің және желілердің тұтастылығы мен қолжетімділігін бұзумен шартталады. Басқалары қылмысты жасаудың не құралы түрінде, не тәсілі ретінде қарастырылады, бірақ оларды тергеудің құқықтық механизмі қылмысты жасаудың адекватты амалы болып табылады.

Түйін сөздер: киберқылмыстылық, халықаралық байланыс, киберқылмыскер, БҰҰ, қылмыстылықпен күресу, халықаралық келісімдер.

УДК 343

*Джансараева Р.Е., Аратулы К.

Казахский национальный университет имени аль-Фараби,
Республика Казахстан, г. Алматы
*E-mail: jansarayeva@mail.ru

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

В соответствии с рекомендациями экспертов ООН термин «киберпреступность» подразумевает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках, а также против компьютерной системы или сети.

Основной целью киберпреступника является компьютерная система, которая управляет разнообразными процессами, и та информация, что циркулирует в них. В отличие от обычного преступника, что действует в реальном мире, киберпреступник не использует традиционное оружие, например, нож или огнестрельное оружие. Его арсенал – информационное оружие, все инструменты, которые используются для проникновения к сети, взлома и модификации программного обеспечения, несанкционированного получения информации или блокировки работы компьютерных систем. К оружию киберпреступника можно прибавить: компьютерные вирусы, программные закладки, разнообразные виды атак, которые делают более возможным и эффективным несанкционированный доступ к компьютерной системе. В арсенале современных компьютерных преступников есть не только традиционные средства, но и самое современное информационное оружие и оборудование. Все проблемы, связанные с раскрытием компьютерных преступлений уже давно пересекли границы государств и получили международное значение [1].

Сегодня обычный рядовой пользователь компьютерной техники и сети может запросто произвести распечатку на принтере документов разного рода, бланков, свидетельств, штампов, сертификатов и т.д. Доказать причастность лица к совершению информационного преступления непросто. Для системной борьбы с преступлениями подобного рода между странами Европы и Азии создаются Национальные контактные пункты. В настоящее время осуществляется постоянный обмен информацией и опытом со странами бывшего СНГ и дальнего зарубежья [2].

Жертвы компьютерной преступности проявляют нежелание контактировать с провоохранительными органами, опасаясь распространения мнения о собственной халатности и ненадежной работе своей фирмы или организации. Кибер-

преступность угражает не только отдельным лицам или организациям, но и потенциально – национальной безопасности любой страны, достигшей значительного уровня компьютеризации жизненно важных отраслей экономики.

Преступления в сфере информационных технологий, как ранее говорилось, нередко являются международными, то есть преступники действуют в одном государстве, а их жертвы находятся в другом государстве. Поэтому для борьбы с такими преступлениями особое значение имеет международное сотрудничество.

Конвенция Совета Европы о преступности в сфере компьютерной информации (ETSN 185) была подписана 23 ноября 2001 года в Будапеште. Она открыта для подписания как государствами-членами Совета Европы, так и не являющимися его членами государствами, которые участвовали в ее разработке. В частности, ее подписали Россия, США и Япония.

Конвенция Совета Европы о киберпреступности подразделяет преступления в данной сфере на следующие группы:

1. Преступления, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем: незаконный доступ (статья 2), незаконный перехват (статья 3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных) или системы (статья 4, статья 5). Также в эту группу преступлений входит противозаконное использование специальных технических устройств (компьютерных программ, разработанных или адаптированных для совершения преступлений, компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерной системе в целом или любой ее части) (статья 6).

2. Преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (статьи 6, 7 и 8). Подлог с использованием компьютерных технологий включает в себя злонамеренные противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных.

3. Производство, предложение или предоставление в пользование, распространение и приобретение детской порнографии, а также владение детской порнографией, находящейся в памяти компьютера (статья 9).

4. Преступления, связанные с нарушением авторского права и смежных прав [3].

Согласно Конвенции каждое государство-участник обязан создать необходимые правовые условия для предоставления следующих прав обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, ее части или носителей; изготовление и конфискация копий компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

Конвенция также требует создать необходимые правовые условия, как обязать Интернет-провайдеров проводить сбор и фиксацию или перехват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

В начале 2002 года был принят Протокол №1 к Конвенции о киберпреступности, добавляющий в перечень преступлений распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица, или группы лиц, основывающегося на расовой, национальной, религиозной или этнической принадлежности.

Во многих странах мира в целях пресечения факта информационного преступления в последние годы специалисты по компьютерной безопасности начали сотрудничество с психологами, которые составляют профиль так называемого хакера, то есть преступника в сфере компьютерной информации и техники, который позволяет выявить уровень его квалификации и технической подготовки. Но следует отметить, что хотя компьютерные специалисты и могут многое сказать о хакере и о методах его работы, но они никогда не смогут понять психологию его криминального мышления. Подобными вопросами занимаются клинические психологи, судебные эксперты и другие специалисты совместно с органами внутренних дел. Подобная практика активно используется в США, Европе и других странах, где киберпреступления широко развиваются. Но ввиду того, что в современных условиях значительная часть средств борьбы с

киберпреступлениями, как и с другими преступлениями международного характера, принадлежит к внутренней компетенции каждого отдельного государства, необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласовывая его с международными нормами права и опираясь на существующий позитивный опыт.

Новые информационные технологии должны быть не только орудием, средством совершения преступлений нарушителями закона, но и должны стать эффективным наступательным инструментом в борьбе с различными угрозами и в том числе преступностью во всех ее проявлениях. В связи с чем нужно привлекать в государственные структуры высококвалифицированных специалистов, которые на равном практическом и квалифицированном уровне могли бы сотрудничать и плодотворно работать, сотрудничая на межгосударственном пространстве по противодействию киберпреступности.

Литература

1 Журнал «Законность и правовая статистика» – интернет-ресурс www.law-cs.com.
2 Голубев В. Стратегия и тактика борьбы с киберпреступностью в странах СНГ. – crime-research.ru. – 2005.
3 «Европейская Конвенция по преступлениям в киберпространстве» от 23 ноября 2001 года.

References

1 Journal «law and legal statistics» – online resource www.law-cs.com.
2 Golubev V. «Strategy and tactics of fighting cybercrime in CIS countries» – crime-research.ru. – 2005.
3 «The European Convention on crime in cyberspace», November 23, 2001.