М.Э. Сакатаева,
старший преподаватель информатики кафедры «Экономические дисциплины»
Академии экономики и права

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ГОСУДАРСТВЕННАЯ ПОЛИТИКА РК В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Научно-техническая революция повлекла за собой серьезные социальные изменения. Наиболее важным из них является возникновение нового вида общественных отношений и общественных ресурсов – информационных. Последние отличаются от известных сырьевых энергетических ресурсов целым рядом особенностей, а именно:

1) они непотребляемы и подвержены не физическому, а моральному износу; 2) по своей сущности они нематериальны и несводимы к физическому носителю, в котором воплощены;

3) их использование позволяет резко сократить потребление остальных видов ресурсов, что в конечном итоге приводит к колоссальной экономии средств; 4) процесс их создания и использования осуществляется особым способом – с помощью компьютерной техники.

Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки, в свою очередь, стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники, средств телекоммуникаций и систем связи.

Все это в целом входит в понятие «новой информационной технологии», которая представляет собой совокупность методов и средств реализации информационных процессов в различных областях человеческой деятельности. С помощью этой технологии происходит реализация информационной деятельности человека, которого самого можно рассматривать как информационную систему. Иными словами, информация становится продуктом общественных (информационных) отношений, начинает приобретать товарные черты и становится предметом купли-продажи. Следствием протекающих в обществе информационных процессов является возникновение и формирование новых социальных отношений и изменение уже существующих. Например, уже сейчас можно констатировать значительный объем договорных отношений, связанных с изготовлением, передачей, накоплением и использованием информации в различных ее формах: научно-технической документации, программного обеспечения, баз данных, систем управления базами данных (СУБД) и других

Однако новые информационные технологии дали толчок не только новому витку научно-технического прогресса общества, но и стимулировали возникновение и развитие новых форм преступности. Революция в области компьютерной техники предоставила преступникам широкие возможности в плане доступа к новым техническим средствам.

Компьютерные преступления можно условно подразделить на две большие категории: а) преступления, связанные с вмешательством в работу компьютеров и б) преступления, использующие компьютеры как необходимые технические средства[1].

---

[1] См.: Згадзай О.Э., Казанцев, С.Я., Казанцева Л.А. Информатика для юристов. – М., 2001. – С. 220.

К преступлениям, связанным с вмешательством в работу компьютеров, относятся:

1) несанкционированный доступ к информации, хранящейся в компьютере, который осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных[1];

2) ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему;

3) разработка и распространение компьютерных вирусов;

4) преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям;

5) подделка компьютерной информации;

6) хищение компьютерной информации.

При рассмотрении второй категории преступлений можно выделить разработку сложнейших математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными – рекомендации по выбору оптимального варианта действий преступника.

Итак, под компьютерными преступлениями следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть, то есть средства электронно-вычислительной (компьютерной) техники.

Средства компьютерной техники можно разделить на две группы:

1. Аппаратные средства – это технические средства, используемые для обработки данных. К ним относятся:

– персональный компьютер;

– периферийное оборудование (комплекс внешних устройств, не находящихся под непосредственным управлением центрального процессора);

– физические носители машинной информации.

2. Программные средства – это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения. К ним относятся:

а) программное обеспечение, в состав которого входят:

– системные программы (операционные системы, программы технического обслуживания);

– прикладные программы (программы, которые предназначены для решения задач определенного типа, например редакторы текстов, антивирусные программы, СУБД и т.п.);

– инструментальные программы (системы программирования, состоящие из языков программирования и трансляторов – комплекса программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды);

---

[1] См.: Никифоров И. Компьютерные преступления. Уголовные меры борьбы с компьютерной преступностью // Защита информации, 1999, №5/3. – С. 145

б) машинная информация владельца, собственника, пользователя.

На основе данных теории и практики борьбы с компьютерной преступностью можно выделить две основные группы мер предупреждения компьютерных преступлений:

1. Правовые. В эту группу мер предупреждения компьютерных преступлений прежде всего относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере. Если обратиться к истории, то мы увидим, что первый нормативно-правовой акт такого типа был принят американскими штатами Флорида и Аризона в 1978 году. Этот закон назывался «Computer crime act of 1978». Затем аналогичные законы были приняты почти во всех штатах Америки. Эти акты стали фундаментом для дальнейшего развития американского и зарубежного законодательства в целях осуществления мер предупреждения компьютерных преступлений[1].

2. Организационно-технические. В комплекс технических средств защиты входят:

– брандмауэр (межсетевой экран) – программная и/или аппаратная реализация;

– системы обнаружения атак на сетевом уровне;

– антивирусные средства;

– защищенные операционные системы, обеспечивающие уровень B2 по классификации защиты компьютерных систем и дополнительные средства контроля целостности программ и данных (Windows XP, Vista и т.д.);

– защита на уровне приложений: протоколы безопасности, шифрования, электронно-цифровая подпись, цифровые сертификаты, системы контроля целостности;

– защита средствами системы управления базами данных;

– защита передаваемых по сети компонентов программного обеспечения;

– мониторинг безопасности и выявление попыток вторжения, адаптивная защита сетей, активный аудит действий пользователей;

– корректное управление политикой безопасности[2].

Зарубежный опыт показывает, что наиболее эффективной мерой в этом направлении является введение в штатное расписание организации или государственного органа должности специалиста по компьютерной безопасности (администратора по защите информации), либо создание специальных служб, как частных, так и централизованных, исходя из конкретной ситуации. Наличие такой службы снижает вероятность совершения компьютерных преступлений во много раз.

Информатизация современного общества и, в частности, повсеместное использование глобальной сети Internet привели к формированию нового вида преступлений – киберпреступлений.

Вот несколько примеров самых громких IT-преступлений, взятых из списка издания GearCrave.

Одну из первых громких хакерских атак совершил в 1983 году американский студент, в будущем и один из самых известных хакеров Кевин Митник. Используя университетский компьютер, он проник в глобальную сеть ARPANet, являющуюся предшественницей Internet, и сумел войти в компьютеры Пентагона. Он получил доступ ко всем файлам Министерства обороны США.

Безусловно, крупнейшим и самым загадочным интернет-преступлением до сих пор остается преступление 1989 года. Неизвестные сумели запустить в компьютерную сеть NASA «червя» WANK, вызвавшего катастрофический сбой в программе. Ситуация

---

[1] См.: Угланов Ю.А. Правовые и организационные вопросы борьбы с преступлениями в сфере компьютерной информации в Российской Федерации**.** Доклад на VII Международной конференции «Право и Интернет»

[2] См.: Хомколов В.. Центр исследования компьютерной преступности. Предупреждение преступлений в сфере компьютерной информации. http://www.crime-research.ru

оказалась настолько серьезной, что запуски нескольких спутников пришлось перенести на другое время.

Ущерб почти 25 миллионов долларов причинили американским банкам два хакера из России. В ноябре 2000 года в США ФБР поймало хакеров из Челябинска: 20-летнего Алексея Иванова и 25-летнего Василия Горшкова. Россиянам удалось взломать компьютерные системы нескольких компаний и украсть номера кредитных карт, в частности они похитили 15,7 тыс. номеров кредитных карт из Western Union.

На протяжении 30 минут в 49 городах мира (включая Нью-Йорк, Москву и Гонконг) с помощью нескольких сотен поддельных пластиковых карт в 137 банкоматах были сняты 9 млн долларов США. Это событие стало крупнейшей кардерской атакой и по организации, и по уровню ущерба. Преступники смогли совершить такую атаку после того, как им удалось взломать компьютерную систему банка RBS WorldPay. Хакеры украли информацию, необходимую для создания пластиковых карт, изготовили эти карты и организовали массовый синхронный съем денег.

Ущерб более чем 300 миллионов долларов нанес компании Dassault Systemes 58-летний хакер из Греции. В январе 2008 года он был арестован местной полицией за незаконное вторжение в серверы компании и кражу программного обеспечения, которое впоследствии вор продал в Интернете.

Анализ этих и подобных происшествий дал основание для неоспоримого вывода: почти все виды компьютерных преступлений можно было так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать различные профилактические меры, под которыми следует понимать деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению.

Усилия по борьбе с компьютерными преступлениями сегодня предпринимаются как на национальном, так и на межгосударственном уровнях. Об этом свидетельствует ряд международных документов, из которых выделяются следующие:

- конвенция о киберпреступности, принятая 27 апреля 2000 года Советом Европы; меры по борьбе против преступлений, связанных с использованием компьютеров, утвержденные XI Конгрессом Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, состоявшемся в Бангкоке 25 апреля 2005 года; Окинавская хартия глобального информационного общества, принятая 23 июля 2000 года в Японии на совещании руководителей глав государств и правительств стран «Группы Восьми».

В масштабе СНГ 17 февраля 1996 года на VII пленарном заседании Межпарламентской ассамблеи был принят Модельный уголовный кодекс, в котором регламентируется ответственность за компьютерные преступления. 1 июня 2001 года в Минске было принято Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации. В России, Украине, Республике Беларусь, Республике Казахстан и в некоторых других государствах – членах СНГ рассматриваемая проблема потребовала от законодателя принятия срочных адекватных правовых мер противодействия данным преступным посягательствам – разработку новых, унификацию и совершенствование ранее принятых законов, иных правовых актов и нормативных документов.

В послании президента народу Казахстана от 10 октября 1997 года «Казахстан — 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев» в качестве долгосрочного приоритета определена национальная безопасность, одной из составляющих которой является информационная безопасность.

В Республике Казахстан закреплена уголовная ответственность за компьютерные преступления, а именно: неправомерный доступ к компьютерной информации, созда-

ние, использование и распространение вредоносных программ для ЭВМ. Данная статья Уголовного кодекса Республики Казахстан относится к разделу преступлений в сфере экономической деятельности. Первоначально она носила название «Неправомерный доступ к компьютерной информации». Однако с развитием рыночных отношений и глобальной компьютеризацией 21 декабря 2002 года парламент Республики Казахстан внес дополнение в статью 227 УК РК, формулировка которой запрещает «неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ».

В системе Министерства внутренних дел с апреля 2003 года создано и функционирует управление «К» (специальная оперативно-аналитическая работа и раскрытие преступлений в сфере высоких технологий) департамента криминальной полиции, занимающееся раскрытием преступлений в сфере высоких технологий.

Одним из основных направлений деятельности подразделений по борьбе с преступлениями в сфере высоких технологий является выявление и раскрытие преступлений в телекоммуникационных и информационных системах:

– борьба с преступлениями, связанными с незаконным доступом к компьютерной информации;

– с незаконным оборотом радиоэлектронных и специальных технических средств; – распространением предметов и информации, запрещенных в свободном обороте (порнографии, контрафактной продукции, вредоносных программ);

– борьба с преступлениями в сфере телекоммуникаций, а также организация работы по использованию возможностей информационно-телекоммуникационных и компьютерных технологий для раскрытия преступлений[1].

В целях реализации положений Конвенции о преступлениях в компьютерной сфере в 2006 году в структуре МВД создан Национальный контактный пункт по борьбе с преступлениями в сфере высоких технологий, который обеспечивает межгосударственное взаимодействие и оперативное реагирование по фактам несанкционированного доступа к компьютерной информации. В настоящее время осуществляется постоянный обмен информацией со странами СНГ и дальнего зарубежья.

10 октября 2006 года был подписан указ президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан». Эта концепция разработана на основании Конституции Республики Казахстан и законов Республики Казахстан, в частности «О национальной безопасности Республики Казахстан» от 26 июня 1998 года, «О государственных секретах» от 15 марта 1999 года, «О борьбе с терроризмом» от 13 июля 1999 года, «Об электронном документе и электронной цифровой подписи» от 7 января 2003 года, «Об информатизации» от 8 мая 2003 года и «О противодействии экстремизму» от 18 февраля 2005 года. Перечисленные нормативные акты создали правовую базу для пресечения преступлений в сфере высоких технологий.

Большое значение в организации борьбы с компьютерными преступлениями имеет и «Концепция развития конкурентоспособности информационного пространства Республики Казахстан на 2006-2009 годы», утвержденная указом президента Республики Казахстан от 18 августа 2006 года №163. При разработке концепции учтены международный опыт в области информационной безопасности и положения «Концепции информационной безопасности государств – участников Содружества независимых государств в военной сфере» от 4 июня 1999 года. Концепция служит основой при формировании и реализации единой государственной политики Республики Казахстан в области обеспечения информационной безопасности, ее положения будут учитываться

[1] См.: Материалы служб органов внутренних дел. Комитет криминальной полиции. Информация о борьбе с преступлениями в сфере высоких технологий. http://www.mvd.kz

при создании и развитии единого информационного пространства Казахстана и дальнейшем совершенствовании государственной политики в области информатизации.

Проблемам компьютерной безопасности и компьютерной преступности должно уделяться особое внимание. Иерархически правильно построенная система доступа к данным на государственном уровне, современное оборудование, штат квалифицированных работников, отвечающих за компьютерную безопасность, – это гарант безопасности государственной информации, а вместе с тем и государства.

Түйін

Мақалада компьютерлік қылмыстылық пен Қазақстан мемлекеті саясатының осы қылмыс түрлерінің алдын алу және онымен күрес жүргізуге қатысты мәселелері қарастырылады. Компьютердің жұмысына араласып кетумен және компьютерді техникалық құрал ретінде пайдаланушылықпен байланысты туындап отырған компьютерлік қылмыс түрлері атап көрсетіледі. Қылмыстың жаңа түрлерінің алдын алу және онымен күрес жүргізу мәселелеріне байланысты осы саладағы трансұлттық достастықтағы мемлекеттерге назар аударылады.

Annotation

The matters of the computer criminality and Kazakhstan policy in the sphere of prevention and struggle with such crimes have been shown in the article. Classification of the computer crimes, connected with the interference into the computer work and crimes using them as technical means has been given. Special attention has been paid to the transnational cooperation of states in this sphere connected with the matters of prevention and struggle with the new types of crimes.