В Республике Казахстан (ч.8 ст.70 УК РК), как и в ст. 69 УК Киргизской Республики, ст. 76 УК Таджикистана установлен запрет на применение условно-досрочного освобождения лицам, у которых смертная казнь заменена пожизненным лишением свободы в порядке помилования. Несомненно, "при таком подходе вот этим-то лицам, лишенным всякой надежды, не нужно никакое воспитательное воздействие, и они будут самыми опасными в период отбывания наказания". [4, 18]

На наш взгляд, позиция УК РФ, который отказался от формальных ограничений применения условно-досрочного освобождения в отношении каких-либо категорий осужденных, является приемлемой и для нашего государства, в связи с этим желательно ч.8 ст. 70 УК РК отменить. Что касается цели частного предупреждения, то мы согласны с тем, что многие из них сами осудят себя за совершенное преступление, и это будет высшей карой. Международные исследования показывают, что лица, приговоренные к пожизненному заключению и впоследствии освобожденные, как правило, не совершают повторных преступлений. Например, в Великобритании королевская комиссия по смертной казни исследовала 129 подобных материалов и установила, что 122 бывших осужденных вели себя хорошо, и лишь один вновь совершил убийство. В Пенсильвании за последние 37 лет из 607 лиц, осужденных пожизненно и условно освобожденных, только один совершил умышленное убийство первой степени. [4 ,20]

Итак, с точки зрения реализации целей уголовного наказания, пожизненное лишение свободы обладает множеством негативных свойств, которые ставят под сомнение саму возможность реализации некоторых целей наказания. Исходя из содержания и установленного законом порядка исполнения наказания для преодоления некоторых противоречивых моментов между теорией и практикой, на наш взгляд, цель пожизненного лишения свободы следует определить следующим образом: Пожизненное лишение свободы применяется в целях установления справедливости и ограждения граждан, общества и государства от особо опасных лиц.

1. Минаков Ю., Тимошенко С. Пожизненное лишение свободы в законодательстве зарубежных стран. Правовое и методическое обеспечение наказаний М, ВНИИ МВД РФ. 1994. С. 62.
2. Ной И. С. Сущность и функции уголовного наказания в советском государстве. Саратов, 1973, - 193 с.
3. Наташев А.Е.. Стручков Н.А. Основы теории исправительно-трудового права. М.. 1967-191с.
4. Посмаков П.Н. Право человека на жизнь и отмена смертной казни в Казахстане. // Фемида №11. 2002 С. 18-20.
5. Письмо КУИС МЮРК за № 14/7 - 1438 от 24.04.03. 10 листов.
6. Кистяковский А.Ф. Исследование о смертной казни. Тула. «Автограф» 2000.

***

Бұл мақалада, өмірбойы қамау жазасын тағайындау кезінде көзделетін мақсаттар мен оларды жүзеге асырудың мәселелері қарастырылған.

***

This article discusses the objectives in imposing the penalty of life imprisonment or problems in its implementation.

К. Аратулы

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РК И ЗАРУБЕЖНЫХ СТРАНАХ

1974 году на рынке появляются компактные, сравнительно не дорогие персональные компьютеры для бесконечного круга пользователей всемирной глобальной сети, что приводит к таким же глобальным изменениям в всех отраслях человеческих отношений. Новые общественные отношения приводят к новым отступлениям от закона, новым видам преступлений, то есть к компьютерным преступлениям [1].

Для уголовно-правовой науки и для законодательства появляется новый предемет научных и политических обсуждений и разработок.А что же является предметом преступлений в сфере компьютерной информации по уголовному законодательству Казахстана. Это те позиций которые базируются в нормах УК РК, регламентирующих отношения, связанные с использованием информации и информационных технологий, проведение анализа этих норм раскрывает всю обширность возможных преступных деяний в сфере новых коммуникационных технологий. Казалось бы, что компьютерную информацию каждый пользователь распространяет, также защищает на бытовом уровне, тем не менее, в соответствии с УК РК компьютерная информация подлежит уголовно-правовой защите, хотя в ограниченной форме.

Основным требованием, предъявляемым к такой информации, применительно к нормам уголовного закона, является то, что такая информация должна быть порядком ограничена в доступе. Все тайны, составляющие информацию с ограниченным доступом, опираясь на триаду «личность,

общество, государство», можно разделить на три категории: личная тайна; семейная тайна, коммерческая тайна, профессиональные тайны; государственная и служебная тайны [2].

Анализ и толкование раздела уголовного кодекса РК преступления в сфере экономической деятельности дают нам бесконечный ряд проблем, как возникающих из-за расширительного и не вполне корректного толкования понятия компьютерной информации как предмета рассматриваемых преступлений, в то же время так и узкого и не конкретного использования таких понятий в самом законодательстве Республики Казахстан. Так, в течение последних лет правоприменительные органы исходя из того, что программа для ЭВМ, записанная на машинный носитель, является компьютерной информацией, поэтому неправомерный доступ к программе на машинном носителе квалифицируется как доступ к информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, или как законодатель утверждает что незаконный доступ повлекший уничтожение, блокирование, модификацию либо копирование, также нарушение компьютерной техники, их сети и системы совершается лицом имеющим доступ к вышеперечисленным объектам карается законом, что приводит к тому, что подобная правоприменительная практика не соответствует действующему законодательству и в полной мере не осуществляется. Неправомерный доступ компьютерной информации может совершать каждый человек, и без права и без возможности доступа к ней, а также не каждый из вышеперечисленных незаконных деяний может привести к их уничтожению, блокированию, модификации и т.д., что даже часто является не обнаруженным ни самими пользователями, ни организациями, ни государством и даже не программным обеспечением, который предназначен для обнаружения таких посягательств. Неправомерный доступом или просто незаконным проникновением должны считаться действия, которые не только привели к уничтожению, блокированию, копированию, модификации или нарушению системы ЭВМ, сети или самой ЭВМ, но и причинили моральный ущерб, нарушили авторские и смежные права, унизили честь и достоинство пользователя или стали препятствием для достижения своих целей рядовыми пользователями, привели к остановке непрерывной роботы, или остались незаметными и необнаруженными, но противоречили правам и законным интересам пользователей. Программа для ЭВМ казалось бы является объектом авторского права, но незаконные действия по отношению к ней не являются неправомерным доступом к компьютерной информации. Пользование программами без лицензии будет нарушением авторских и смежных прав создателей программ, и эти нарушения прямого отношения к неправомерному доступу не имеют, а вот то, что хранится в программе или с помощью программы ЭВМ является объектом хищения путем неправомерного доступа к компьютерной информации, и в то же время может быть объектом авторского права [3].

Компьютерные технологий и услуги связанные с ними стали неотъемлемой частью жизнедеятельности всего человечества. На практике зачастую многие противоправные деяния совершаются с использованием компьютерной техники или новой технологии где используются компьютерные программы либо компьютерная информация, что безусловно приводит к мысли что неправомерный доступ к компьютерной информации, к ЭВМ, системе и сети ЭВМ может играть роль метода, средства, предмета, а чаще всего и способа совершения преступлений. Поэтому несанкционированный доступ к компьютерной сети, информации и системе как одного из групповых признаков совершения преступлений, как понятия общепреступного характера можно отнести к общей части изучения уголовного законодательства и права. А в особенную часть уголовного закона инкриминировать и пенализировать целый ряд преступных составов связанных с компьютерной информацией, а с последующим развитием новых технологий и полной разработкой методологических и теоретических вопросов данной отрасли выделить и целый раздел, посвященный компьютерной информации и всей системе ЭВМ.

В международных отношениях разных стран рассматриваются различные подходы к пониманию преступлений в сфере компьютерной информации, их соотношение с понятием компьютерных преступлений, киберпреступлений, преступлений в сфере высоких технологий. В 2000 году американские ученые провели глобальное исследование уголовного законодательства 52 стран и пришли к выводу, что в тех странах, в которых предусмотрены преступления, совершаемые в «информационном пространстве» (cyberspace), можно выделить 10 видов таких преступлений, объединенных в четыре категории:

1. преступления, связанные с информацией, включая ее перехват, модификацию и кражу;

2. преступления, связанные с компьютерными сетями, включая вмешательство в их работу и саботаж;

3. преступления, связанные с доступом, включая хакерство и распространение вирусов; а также

4. преступления, связанные с использованием компьютеров, включая оказание помощи и соучастие в преступлении, компьютерное мошенничество и компьютерный подлог.

Принимая во внимание результаты научных исследований и законодательную практику различных государств, а также международного сообщества, к числу компьютерных преступлений можно отнести преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационных технологий. В зависимости от объекта и предмета посягательства все компьютерные преступления, предусмотренные как в отечественном, так и зарубежном уголовном праве, можно разделить на две группы:

1. Преступления в сфере компьютерной информации. Предметом в таких преступлениях выступает компьютерная информация, как, например, в деяниях, предусмотренных статьями 227 УК РК, 272-274 УК РФ, статьями 361-363 УК Украины, §1030 (a)(1) Свода Законов США «Несанкционированный доступ к информации с ограниченным доступом, касающейся национальной безопасности, международных отношений, атомной энергетики», статьей 478.1 УК Австралии «Несанкционированный доступ или модификация охраняемой компьютерной информации или программы» и рядом других.

2. Преступления, где компьютерная информация является орудием или средством совершения другого преступления. Эти составы преступлений находятся в других главах уголовных кодексов, к примеру, в статье 212 УК Республики Беларусь «Хищение путем использования компьютерной техники»; §1030(a)(7) Свода Законов США «Вымогательство, угрозы причинения вреда с использованием компьютера»; статье 206(1)(e) УК Канады «Использование компьютерных данных и технологий в целях извлечения прибыли путем создания финансовых пирамид» и других. А поуголовному кодексу РФ, ответственность за преступления этой группы должна наступать по иным статьям Кодекса в соответствии с их родовым и непосредственным объектами. Однако такие деяния в необходимых случаях могут квалифицироваться по совокупности с преступлениями, предусмотренными статьями 272-274 УК РФ. В Республике Казахстан, к сожалению, статей уголовного кодекса, где упоминается использование компьютерной техники или их дополнительных устройств, нет.

Целый ряд преступлений подобного рода приводится в примере научной работы У.В.Зининой, а также в работах А.Т.Нугмановой и Т.Б.Сеитова [4].

С недостаточными отечественными научными трудами, анализом в сфере компьютерной информации, есть необходимость рассмотрении зарубежных специальных научных трудов и научной литературы, книг и пособий. На основе анализа можно выделить более 20 способов совершения компьютерных преступлений и около 40 разновидностей преступных деяний, относящихся к киберпреступлениям. Эти цифры могут меняться в сторону роста в зависимости от типовых признаков до общих, от комбинации совершения преступлений преступниками, от развития новых технологий, а также от логической модификации алгоритмов преступных деяний.

В связи с этим компьютерные преступления можно подразделить на 5 основных групп, что и сделал знаменитый ученый-юрист, автор многих монографий и научных трудов, а также диссертации, посвященной к компьютерной преступности Ю.М.Батурин. К этим основным группам относятся:

1) хищение компьютерных технических устройств и приборов;
2) копирование и перенаправление компьютерной информации;
3) незаконный доступ к компьютерным техническим устройствам;
4) манипуляция информационными и управляющими командами;
5) деяния с использованием комплексных способов [5].

На отчественной арене хороший комплекс способов и видов совершения преступлений приводит Президент РК в своей концепции информационной безопасности, что на данный момент своего практического продолжения в дастаточной мере не нашло. В Указе Президента РК «О концепции информационной безопасности Республики Казахстан» от 10 октября 2006 года приведены понятия, способы совершения преступлений и преступные деяния ранее не указанные в полной мере ни в Уголовном кодексе РК, ни в одном научном труде отечественных деятелей.

Из большого списка способов, методов, видов совершения преступлений в сфере копьютерной информации можно выделить несколько основных:

1) несвоевременная информационная переписка либо ошибка адреса, незаконное собирание и использование информации;
2) неправомерный доступ к информации и информационным ресурсам, уничтожение, модификация и копирование компьютерной информации против закона;
3) незаконная манипуляция информацией или воздействие на информацию (дезинформация, изменение либо сокрытие информации);
4) незаконное копирование текстов в информационных системах;

5) пользование СМИ против интересов человека, общества и государства;
6) хищение информации из библиотек, архивов и базы данных;
7) нарушение технологии обработки информации;
8) создание и распространение программ вирусов;
9) установление программных и информационных периферийных устройств;
10) уничтожение и нарушение устройств обработки связи и информации;
11) уничтожение, нарушение и хищение машинных и других информационных носителей;
12) хищение криптографических средств защиты информации, кража программных или информационных ключей, паролей;
13) отправка, дешифровка и перенаправление ложной информации в коммуникационных сетях и линиях связи;
14) умышленное или небрежное предложение пользователям ложной, неполной либо неправильной информации;
15) и другие противоправные действия в сфере компьютерной информации [6].

В зарубежном и международном уголовном законодательстве при описании сходных составов преступлений употребляется термин «несанкционированный доступ». По мнению многих ученых юристов данный термин является более точным для характеристики запрещенного уголовным законом действия, поскольку правомерность доступа к информации фактически означает его санкционированность (разрешенность) обладателем информации.

Выделяется несколько способов неправомерного доступа к компьютерной информации: способы непосредственного доступа; способы опосредованного (удаленного) доступа; смешанные способы доступа. Во всем мире доля преступных деяний, совершаемых путем удаленного доступа к ЭВМ, системе или компьютерной сети, в общем числе компьютерных преступлений продолжает неуклонно расти и составляет по оценкам специалистов примерно 39,2% [7].

Как примеры из судебной практики, показывают, что незаконное подключение к сети Интернет следственными и судебными органами часто квалифицируется как преступление по статье 227 УК РК, но только с использованием удаленного доступа. При подключении к сети Интернет происходит использование чужого имени пользователя и пароля, поэтому считается, что этот доступ является неправомерным. В то же время, многие авторы, исследовавшие эту проблему, не согласны с подобным подходом в правоприменительной практике. В подобных случаях незаконное подключение к сети Интернет приводит к изменению статистической информации в биллинговой системе. Биллинговая система (т.е. автоматизированная система расчетов) представляет собой программно-аппаратный комплекс, предназначенный для учета потребления услуг связи, управления расчетами за такие услуги, управления самими услугами одновременно с хранением информации об абонентах, которым оператор связи оказывает эти услуги [8].

Сама по себе автоматизированная система не может определить, правомерно или нет тот или иной субъект ввел данные абонента. Таким образом, в официальную статистику преступности в сфере компьютерной информации включаются случаи не вполне корректного применения правоприменительными органами уголовного закона, свидетельствующие о расширительном толковании элементов состава преступления, предусмотренного уголовным законом РК, а также недостаточном непонимании технических условий функционирования телекоммуникационных сервисов. На сегодняшний день наиболее распространенными видами вредоносных программ являются: компьютерные вирусы, троянские программы, сетевые черви. Также в этой системе есть так называемые зомби–компьютеры, которые представляют собой зараженные компьютеры, предоставляющие неограниченный доступ для неавторизованных и удаленных пользователей (хакеров), позволяя им рассылать с зараженных компьютеров спам или осуществлять скоординированные Dos-атаки на различные интернет-сайты или информационные системы. По оценкам специалистов, в настоящее время более 50% всего спама рассылается при помощи зомби-сетей. В 2007 г. количество зомби–компьютеров выросло на 29% по сравнению с 2006 г., составив около 6 млн., а численность контролирующих их серверов, наоборот, снизилась [9].

В уголовных законах ряда стран СНГ и Прибалтики, также как Казахстана, а также и многих других европейских государств, вообще не предусмотрено такое преступление как нарушение правил эксплуатации ЭВМ (например, в Великобритании, США, Японии, , Эстонии и других). С объективной стороны рассматриваемое преступление состоит в нарушении правил эксплуатации ЭВМ, их системы или сети, т.е. в неисполнении либо в ненадлежащем исполнении правил, которыми должно руководствоваться лицо, имеющее доступ к ЭВМ. Нарушение правил может быть совершено как в форме действия, так и бездействия, например, выражаться в несоблюдении правил, установленных для обеспечения нормального функционирования ЭВМ. Существуют два вида таких

правил: 1) правила, которые разрабатываются изготовителями ЭВМ и поставляются вместе с ЭВМ; 2) правила, которые устанавливаются обладателем информации или оператором информационных систем.

Рост компьютерной преступности, включая преступления в сфере компьютерной информации, и необходимость согласованного подхода государств к выработке уголовно-правовых и уголовно-процессуальных процедур, направленных на борьбу с ней, привели к созданию в 1997 году Комитетом Министров Совета Европы Комитета экспертов по преступности в киберпространстве. По результатам этой работы в 2000 году был разработан проект Конвенции Совета Европы по киберпреступности. Конвенция была открыта к подписанию до 23 ноября 2001 году в Будапеште, и вступила в силу 18 марта 2004 году. По состоянию на 7 апреля 2007 года Конвенцию ратифицировали 19 государств. Европейская Конвенция по киберпреступности является комплексным документом, содержащим нормы различных отраслей права: уголовного, уголовно-процессуального, авторского, гражданского, информационного. В Конвенции не дается определения понятия «компьютерное преступление» или «преступление, связанное с использованием компьютерных технологий», которые использовались в принятых ранее международных документах. В документе используется понятие «киберпреступление», содержание которого раскрывается с помощью перечня, включающего в себя: 1) деяния, направленные против компьютерной информации (как предмета преступного посягательства), 2) деяния, посягающие на иные охраняемые законом блага, при этом информация, компьютеры и т.д. являются одним из элементов их объектив- ной стороны, выступая в качестве, к примеру, орудия их совершения либо составной части способа их совершения или сокрытия.

Данную Конвенцию январе 2006 года ратифицировала Франция, затем в сентябре 2006 года США, Казахстан как и Россия ратификацию Конвенции отложил на более позднее время [10].

На сегодняшний день при выработке согласованных мер противодействия компьютерным преступлениям особое внимание на международном уровне уделяется следующим вопросам: а) обнаружение и идентификация нарушителя, совершившего компьютерное преступление; б) получение доступа к содержанию передаваемых сообщений; в) международное сотрудничество в области сбора доказательств и помощь в случае, если сотруднику правоохранительных органов из одной страны требуется доступ к компьютеру в другой стране для получения доказательств (т.е. «трансграничные оперативно-розыскные мероприятия»); г) налаживание сотрудничества между государственными органами и соответствующими заинтересованными представителями бизнес сообщества (например, интернет-провайдерами). Группой Восьми в 2000 году был принят План действий из 10 основополагающих пунктов по противодействию компьютерной преступности, который, среди иных мер, предусматривал рассмотрение вопросов, связанных с компьютерной преступностью, при подготовке соглашений о правовой помощи, а также рассмотрение методов сохранения электронных доказательств и их представления в рамках иностранного уголовного судопроизводства.

1. Компьютерные преступления и обеспечение безопастности ЭВМ. Проблемы преступности в капиталистических странах. – Москва: Винити, 1983. – №6. – с. 3.

2. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. // Диссертация на соискание учёной степени к.ю.н. – Москва, 2007.

3. Уголовный кодекс РК, принятый 16 июля 1997 года, Особенная часть, статья 227.

4. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане: Учебное пособие. // Алматы: Данекер, 1999. – с. 14.

5. Батурин Ю.М. Компьютерные преступления и компьютерная безопасность. // Москва: Юридическая литература, 1991.

6. Указ Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан» от 10 октября 2006 года, № 199.

7. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве. //Диссертация на соискание учёной степени к.ю.н. – Москва, 2007.

8. Голубев В.А., Головин А.Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий. // www.crime-research.org /articles.

9. www.computerra.ru/news/31134025

10. www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm 30

***

In given article the analysis and interpretation domestic criminally-rules of law, and also practice of foreign countries on struggle against crimes in sphere of the computer information and technics is given. Contradictions of practical actions with effective standards of legislation are described, examples from foreign scientific works with use of the statistical data are resulted. The done works and their forthcoming problems this sphere in the international communities, the organizations and foreign countries reveal.

***