**РЕФЕРАТ**

На тему: Уголовное законодательство зарубежных стран об ответственности за несанкционированный доступ к компьютерной информации

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ

Уголовное законодательство зарубежных стран об ответственности за несанкционированный доступ к компьютерной информации

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

**ВВЕДЕНИЕ**

Для эффективной борьбы с компьютерными преступлениями, в частности с несанкционированным доступом к компьютерной информации, необходимо учитывать опыт других государств, поскольку данный вид преступлений является новым в отечественном уголовном законодательстве. Вместе с тем проблема борьбы с несанкционированным доступом к компьютерной информации как одним из самых распространенных преступлений в настоящее время остро стоит перед многими зарубежными государствами. Во многих странах идет процесс совершенствования законодательства, регулирующего борьбу с компьютерной преступностью. Рост компьютерных преступлений, имеющих международный характер, и все более возрастающая угроза от этих преступлений в первую о череде информационной и экономической безопасности вызывают необходимость унификации законодательства в этой области. С этой целью был проведен сравнительно-правовой анализ уголовного законодательства ряда зарубежных стран с целью выявления общих и отличительных особенностей

установления уголовной ответственности за несанкционированный доступ к компьютерной информации.

Законодательство об уголовной ответственности за несанкционированный доступ в различных странах мира существенно различается. Не во всех государствах оно в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны правоотношений, связанных с использованием компьютерных технологий и информации. Изучение накопленного в других странах законодательного опыта позволит выработать предложения по совершенствованию Уголовного кодекса (далее - УК) Республики Беларусь в части обеспечения безопасности использования' компьютерной информации.

**Уголовное законодательство зарубежных стран об ответственности за несанкционированный доступ к компьютерной информации**

Системный анализ УК 17 зарубежных государств по изучению опыта криминализации несанкционированного доступа позволяет сделать следующие выводы.

Несанкционированный доступ в том или ином виде в зависимости от формы выражения законодательно закреплен во всех изученных нами УК. Позиции зарубежных законодателей в отношении криминализации несанкционированного доступа можно представить в виде трех групп.

К первой группе отнесем позиции законодателей Австралии, Австрии Бельгии, Дании, Франции, которые в УК закрепили самостоятельный состав несанкционированного доступа. Ко второй группе отнесем позиции создателей УК Кореи, Испании, Норвегии, Швеции, Швейцарии, в которых несанкционированный доступ выступает в качестве способа совершения других преступлений. В третью группу, полагаем, следует отнести УК Польши, Голландии, ФРГ, Турции, где законодатели закрепили несанкционированный доступ не только в качестве самостоятельного состава, но и предусмотрели его в качестве способа совершения других преступлений.

Представляет интерес анализ объективных и субъективных признаков состава несанкционированного доступа.

Исходя из расположения несанкционированного доступа в УК зарубежных государств, можно сделать вывод, что законодатели по-разному подходят к определению родового объекта этого преступления. В большинстве из изученных нами УК таковыми «выступают общественный порядок (Голланди.4, КНР, Норвегия), неприкосновенность системы автоматизированной обработки информации (Бельгия, Франция), частная сфера и профессиональная тайна (Австрия, ФРГ и др.). В некоторых УК вообще отсутствует указание на родовой объект, так как соответствующая глава носит название «Компьютерные преступления» (Австралия). Таким образом, в зарубежном уголовном законодательстве объектом несанкционированного доступа выступают различные группы общественных отношений, нет единого законодательного подхода к его определению.

При изучении объективных признаков особое внимание необходимо обратить на особенности, характеризующие объективную сторону несанкционированного доступа. Здесь можно отметить следующее. Во-первых, формулировка состава преступления в УК зарубежных государств позволяет говорить о двух вариантах - о доступе к компьютерной информации (Польша, Дания, Норвегия), данным (Австрия, Турция) или сведениям (ФРГ) и о доступе в систему обработки информации (компьютерное устройство, информационную систему) в УК Бельгии, Австрии, Голландии, КНР, Франции, Швейцарии. В последнем случае, что следует из текста соответствующих статей, преступник все равно преследует цель ознакомления с данными (информацией), которые в этой системе находятся. Поэтому, полагаем, целесообразно употреблять словосочетание “доступ к компьютерной, информации”, поскольку несанкционированный доступ к компьютерной системе, по сути, является иным преступлением, которое в международном законодательстве выделяется в отдельный состав.

Во-вторых, по-разному сформулированы в зарубежных УК и обстоятельства совершения несанкционированного доступа. Так, в УК Австрии, Голландии, Норвегии, Польши обязательным признаком объективной стороны является способ – с нарушением системы (мер) защиты; в УК Дании, Турции, КНР указано, что этот доступ является незаконным, противоправным, в УК Бельгии и штата Техас – без разрешения. В УК ФРГ И КНР указано на особо охраняемый характер сведений, которые выступают в качестве предмета доступа. Примечательно, что в большинстве УК соответствующие статьи не содержат наименования указанного в них преступления, но в УК Австрии данное преступление называется противозаконным доступом, в УК Австралии — неуполномоченным доступом, в УК ФРГ — разведыванием сведений.

В-третьих, в зависимости от указания в УК возможных последствий несанкционированного доступа можно говорить о том, что в большинстве случаев основной состав данного преступления сформулирован как формальный (Бельгия, Дания, Голландия и др.).

Анализ субъективных признаков составов несанкционированного доступа, закрепленных в УК зарубежных государств, показывает следующее. По отношению к субъективной стороне можно говорить, что в 100 % изученных нами УК имело место указание на умышленную форму вины. Таким образом, можно говорить о практически полной унификации уголовного законодательства в этом плане. Неосторожная форма вины встречается гораздо реже в квалифицированных составах несанкционированного доступа, причем альтернативно с умышленной формой вины (УК Бельгии).

Что же касается субъекта изучаемого преступления, то таковым в большинстве случаев является физическое вменяемое лицо. А вот в отношении возраста привлечения к уголовной ответственности за несанкционированный доступ к компьютерной информации зарубежные законодатели также не достигли единства, что связано с различными подходами в установлении возраста уголовной ответственности в целом. Так, с 14 лет предусмотрена ответственность в Корее, Австралии; с 15 лет — в Норвегии, Швеции, Дании, Турции, штате Техас; с 16 лет — в КНР, Голландии; с IV лет - в Польше. При этом в некоторых государствах предусмотрена возможность привлечения к ответственности и в более раннем возрасте при условии совершения преступления умышленно. Так, в УК Швейцарии этот возраст установлен с 7 до 15 лет, с 10 до 14 лет - в УК Австралии, с 11 до 15 лет - в Турции, с 12 до 16 лет — в Голландии. Кроме того, в УК Бельгии, Австралии, Франции, Дании, Норвегии установлена и ответственность юридических лиц. Причем, например, в УК Франции в рамках главы, посвященной посягательствам на систему автоматизированной обработки данных, не только указывается на возможность привлечения к уголовной ответственности в рамках данной главы юридических лиц, но и подробно прописан перечень наказаний, которые могут применяться к юридическим лицам за совершение указанных преступлений.

Анализируя квалифицирующие признаки несанкционированного доступа, закрепленные в УК зарубежных государств, можно сказать следующее. Ряд УК (Австрия, Австралия, КНР, Швейцария) содержат только основной состав несанкционированного доступа, не имеющий квалифицированных видов. В то же время в других УК содержится ряд квалифицирующих признаков, среди которых чаще встречаются следующие: несанкционированный доступ с намерением совершить обманную операцию (с целью получить незаконный доход), с использованием служебного положения (превышением полномочий), причинивший определенный ущерб, повлекший изменение или уничтожение данных, с целью изъятия (копирования) данных. Среди иных квалифицирующих признаков можно указать такие, как несанкционированный доступ, совершенный повторно, организованной группой, по приказу, повлекший ухудшение функционирования компьютерной системы. Таким образом, можно сделать вывод, что и квалифицированные виды несанкционированного доступа весьма разнообразны.

Для полной характеристики несанкционированного доступа имеет важное значение и анализ санкций, предусматривающих наказание за преступление с основным составом в УК зарубежных государств. В 92 % санкции являются альтернативными и относительно определенными. Следует отметить, что значительная часть УК предусматривает в санкциях за данное преступление два вида наказания максимальное количество наказаний — три, и только в УК Австралии указан один вид наказания. Причем в подавляющем большинстве (за исключением УК КНР) в качестве одного из наказаний предусмотрен штраф, причем в УК Бельгии, Австрии и штата Техас указаны размеры штрафа. В качестве альтернативы штрафу чаще других предусмотрено тюремное заключение. Причем в отношении этого вида наказания следует отметить следующее. В некоторых УК законодатели предусмотрели срок лишения свободы до 6 месяцев (Австрия, Голландия, Дания, Норвегия) или до 1 года (Бельгия, Франция). Таким образом, законодатели данных стран отнесли несанкционированный доступ к преступлениям, не представляющим большой общественной опасности (как они понимаются в УК Республики Беларусь). В других УК законодатели установили срок лишения свободы до 3 лет (КНР, ФРГ, Турция, Польша), т.е. в этих государствах общественная опасность данного преступления повышена, и его можно относить к категории менее тяжких. Выделяется в этом плане УК штата Техас, размер лишения свободы в котором установлен в зависимости от размера причиненного ущерба и варьируется от 180 дней лишения свободы за основной состав до 99 лет лишения свободы за особо квалифицированный состав несанкционированного доступа (ущерб на сумму свыше 200 000 долларов). Среди других наказаний встречаются арест (КНР), ограничение свободы (Польша).

Хотелось бы также дополнительно остановиться на характеристике уголовного законодательства некоторых зарубежных государств в части установления ответственности за несанкционированный доступ.

Соединенные Штаты Америки являются страной, где компьютерная преступность появилась несколько раньше, чем в других государствах. В связи с этим США и являются одной из первых стран, принявших меры по установлению уголовной ответственности за компьютерные преступления. В 1977 году в США был разработан законопроект о защите федеральных компьютерных систем. Он предусматривал уголовную ответственность за введение заведомо ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации и нарушение этих процессов; хищение денежных средств, ценных бумаг, имущества, услуг, ценной информации, совершенные с использованием возможностей компьютерных технологий или с использованием компьютерной информации.

Указанный закон послужил основой для принятия в октябре 1984 года Закона о мошенничестве и злоупотреблении с использованием компьютеров, который предусматривает в качестве преступлений, в том числе, следующие действия: несанкционированный доступ к правительственным компьютерам; несанкционированный доступ к компьютерам с целью дальнейшего злонамеренного мошенничества; причинение компьютерам повреждения как в результате несанкционированного доступа к нему, так и в результате размещения в нем программ, кодов или информации.

Кроме этого документа в США был принят еще ряд законов (в 1986. 1994, 1996) годах, запрещающих несанкционированный доступ к компьютерной информации в зависимости от ее содержания и значения.

Однако законодательство о компьютерных преступлениях в США не унифицировано. Ответственность за несанкционированный доступ в том или ином виде установлена как в федеральном законодательстве, так и в законодательстве штатов.

В Великобритании преступность деяний непосредственно в сфере компьютерной информации установлена в 1990 году Законом о злоупотреблении компьютерами. В соответствии с ним к уголовно-наказуемым отнесены: умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам; умышленный противозаконный доступ к компьютеру или содержащимся в нем компьютерной информации или программам для их последующего использования в противозаконных целях; неправомерный доступ к компьютерной информации на машинном носителе в компьютере, компьютерной системе или сети, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы компьютера, компьютерной системы или сети. В данном случае несанкционированный доступ к компьютерной информации подвергся разделению на отдельные преступления в зависимости от целей и намерений преступника. Подобные деяния признаются малозначительными и наказываются тюремным заключением до 6 месяцев или штрафом.

Особенность уголовно-правового регулирования ответственности за несанкционированный доступ в Великобритании заключается в установлении ее в статутах, принятых Парламентом Их можно разделить на две основные группы: статуты, устанавливающие ответственность за компьютерные преступления (computer crime), и статуты, устанавливающие ответственность за преступления, связанные с использованием Интернета (internet-related crime).

Следует отметить, что государства англо-американской семьи (системы общего права) в определенной мере восприняли законы США и Великобритании в качестве отправной точки для формирования собственного законодательства об уголовной ответственности за компьютерные преступления. Однако правовое регулирование в этой сфере не отличается единообразием.

Как и европейские страны, государства Азии также не едины в принципах установления уголовной ответственности за несанкционированный доступ к компьютерной информации. Некоторые из них в условиях отсутствия достаточного собственного опыта регулирования по вопросам уголовной ответственности за компьютерные преступления используют в качестве образца законодательство США. К таким государствам относится, например, Республика Филиппины. Криминализация деяний, посягающих на сферу компьютерных информации и пространства, была осуществлена путем принятия Закона о злоупотреблении компьютерами в 2000 году. Законом запрещено умышленно осуществлять несанкционированный доступ к компьютеру, компьютерной сети, компьютерной системе, серверу или базе данных и получать информацию, перечень которой определен законом; умышленно получать несанкционированный доступ к закрытым компьютерам государственных органов или агентств, если такие действия повлекут за собой нарушения в использовании соответствующих компьютеров; с целью совершения мошенничества умышленно осуществлять доступ к защищенным компьютерам без разрешения или с превышением условий данного разрешения в интересах получения значимой информации.

В Малайзии действует Закон о компьютерных преступлениях 1997 года, которым установлена уголовная ответственность за несанкционированный доступ к компьютерным данным; несанкционированный доступ к компьютерным данным с целью совершения иного преступления.

Анализ вышеназванных зарубежных нормативных правовых актов показал, что практически в каждом из них существует указание на несанкционированный доступ к компьютерной информации. И хотя признаки состава этого преступления в УК разных государств описаны по-разному, смысл заключается в запрете несанкционированного доступа к компьютерной информации или компьютерному оборудованию. Указанный запрет независимо от степени описания объективных и субъективных признаков призван охранять безопасность использования компьютерной информации. В то же время анализ показал, что данные различия могут носить существенный характер. Поскольку несанкционированный доступ относят к международным транснациональным преступлениям, то, несомненно, для успешного противодействия этому преступлению необходимо применять единообразные законодательные подходы к установлению уголовной ответственности за него. В настоящее время можно отметить лишь некоторые схожие черты, характерные, как правило, для стран-соседей. Среди возможных путей решения этой проблемы видится выработка совместных договоренностей на международном уровне. В таком случае, возможно, будет говорить о перспективах сближения белорусского и зарубежного законодательства, выработке единых критериев криминализации несанкционированного доступа с целью дальнейшей успешной борьбы с данным и другими видами компьютерных преступлений

**ЗАКЛЮЧЕНИЕ**

Проведенный анализ УК зарубежных государств выявил некоторые заслуживающие внимания особенности. Во-первых, это отсутствие указания на наступление возможных последствий, что позволяет относить во многих государствах данный состав к формальным. Во-вторых, это указание на умышленную форму вины.

Таким образом, несмотря на то, что несанкционированный доступ нашел законодательное закрепление в уголовном законодательстве многих зарубежных государств, отсутствует унифицированный подход к описанию признаков состава данного преступления. Отсутствие единообразного подхода к криминализации несанкционированного доступа не способствует эффективному противодействию данному преступлению.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

1. Роговский, Е.А. Кибербезопасноеть и кибертерроризм / Е.А.Роговский // США - Канада: экономика, политика, культура. - 2003. - № 8 (404). - С. 23-41,
2. Ваганов, П.А. Правовая защита киберпростарнства в США / П.А.Ваганов // Правоведение. -2006. -№4, -С;73-88.
3. Ястребов, Д.А. Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) / Д.А.Ястребов // Государство и право. -2005. -№ 1,-С.! 53-63.
4. Волеводз, А.Г, Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г.Волеводз.- М,: Юрлитанформ, 2002. - 496 с,
5. Уголовное право зарубежных государств. Особенная часть: учеб. пособие / под ред. А.Д.Козочкина; - М.: Камерон, 2004 - 528 с
6. Степанов-Егиянц, В.Г. Ответственность за компьютерные преступления / В.Г.Степаиов-Егиянц // Законность. - 2005. - № 12 - С, 48-49.