

своевременно извещена надлежащим образом о времени и месте рассмотрения дела или по другим причинам не могла представить в суд свои объяснения; рассмотрение дела относится к исключительной компетенции суда в Республике Беларусь и др.

Обращение в Международный коммерческий арбитраж (МКА) – наиболее распространенный способ рассмотрения международных экономических споров. Он является на сегодняшний день эффективным инструментом по урегулированию вопросов, представляя собой особую структуру негосударственного разрешения частных споров, в которой присутствуют иностранные субъекты. Исполнение его решений тщательно проработано на международном и национальном уровне.

*Головенчик М. Г.*

### **К ВОПРОСУ О ПРИЗНАКАХ КИБЕРПРЕСТУПЛЕНИЯ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ НАУКИ И ТЕХНОЛОГИЙ**

*Головенчик Марина Геннадьевна, магистрант Белорусского государственного университета, Минск, Беларусь, marina.golovenchik@inbox.ru*

*Научный руководитель: канд. юрид. наук, доцент Старовойтов О. М.*

Сегодняшние реалии таковы, что современное общество практически ежедневно подвергается различного рода «цифровым атакам», получившим общее понятие «киберпреступление». В российской литературе предпринято немало попыток его формулировки. Так, можно встретить упоминания о них как о «преступлениях в сфере высоких компьютерных технологий» (А. В. Аносов), «преступлениях в телекоммуникационных сетях» (Е. А. Сычев), «компьютерных преступлениях» (А. А. Турышев) и др.

Большинство российских исследователей, к числу которых можно отнести А. И. Халиуллина, Л. Т. Тропину, И. Г. Чекунова и др., сходятся во мнении, что «компьютерным» будет считаться преступление, целью которого является причинение вреда информационной безопасности, если оно совершается с использованием компьютерной системы или сети. Принципиально значимым называют вопрос о режиме совершения данного противоправного деяния – «online» или «offline». При этом делается вывод о том, что, будучи совершаемыми «online», киберпреступления являются составной частью компьютерных преступлений, но не ограничивают последние. Таким образом, первым из значимых признаков киберпреступлений является их совершение посредством использования специальных компьютерных или иных информационно-телекоммуникационных сетей. Данный признак следует отнести к группе уголовно-правовых признаков, поскольку он характеризует обстановку совершения преступления.

Следующим уголовно-правовым признаком киберпреступлений называют их многообъектность. При этом некоторыми исследователями (Е. Н. Карбанова, А. А. Турышев и др.) отмечается, что основным непосредственным объектом рассматриваемых преступлений являются отношения, посредством которых обеспечивается информационная безопасность. В качестве факультативного объекта рассматриваются «связанные с ними общественные отношения». Вместе с тем классическая теория уголовного права придерживается точки зрения, что ранжирование объектов в многообъектных преступлениях следует осуществлять в зависимости от целей, на достижение которых было направлено преступное деяние виновного лица. В связи с этим отношения, обеспечивающие информационную безопасность, будут являться не основным, а дополнительным объектом рассматриваемого преступления.

Характерным уголовно-правовым признаком киберпреступления является способ его совершения. Его наличие следует констатировать тогда, когда модификация информации происходит в такой компьютерной сети, которая имеет непосредственное подключение к другим (конечным) программно-техническим устройствам и (или) по ней распространяется вредоносная компьютерная программа (цифровой код), выступающая, в свою очередь, орудием или средством совершения преступления. Такой способ предложено называть электронным способом совершения преступлений.

С субъективной стороны преступления рассматриваются как умышленные. При этом умысел лица может быть как прямым, так и косвенным.

В литературе встречаются и иные свойства, которыми следовало бы наделить киберпреступления. В частности, российский автор И. Г. Чекунов указывает на следующие факторы: киберпреступления совершаются в особом виртуальном пространстве, а потому с точки зрения географической районизации они являются трансграничными; киберпреступления, как правило, совершаются тайно, что характеризует их как преступные деяния, совершенные в условиях неочевидности; совершение киберпреступлений может осуществляться как посредством разовой атаки, так и вследствие долговременного негативного воздействия на компьютерную сеть (сюда чаще всего относят рассылку нежелательной корреспонденции (спам), DoS- или DDoS-атаки и др.); в ходе совершения киберпреступлений возможно негативное воздействие как из единичного источника, так и из их множества; в качестве преступной мотивации при совершении киберпреступлений могут выступать не только корыстные побуждения, но и иные устремления виновного, в том числе политические мотивы, месть и т. д. Данные признаки, без сомнения, представляют значительный интерес, однако они в большей степени применимы не для уголовно-правовой оценки содеянного, а для его криминологической характеристики и разработки криминалистических методик противодействия киберпреступности.

Таким образом представляется возможным сформулировать следующее определение: «Киберпреступление – это умышленное противоправное деяние, совершаемое в локальной или глобальной компьютерной или иной информационно-телекоммуникационной сети, связанное с несанкционированным размещением, хранением, получением или использованием содержащейся там информации». При этом нельзя не сказать, что само понятие киберпреступления является собирательным, поскольку основными характерными чертами, присущими такому преступлению, остаются способ и обстановка его совершения. Таким образом, проанализировав белорусское законодательство, видится целесообразным внести дополнения в ст. 64 Уголовного кодекса Республики Беларусь, закрепив электронный способ совершения преступления в качестве самостоятельного обстоятельства, отягчающего уголовную ответственность за совершенное преступление.

***Денисенко Р. В., Епифанова Т. О.***  
**ЗАВЕРЕНИЯ ОБ ОБСТОЯТЕЛЬСТВАХ**

*Денисенко Роман Всеволодович, Епифанова Татьяна Олеговна, студенты  
4 курса Южного федерального университета, г. Ростов-на-Дону, Россия,  
lawyer.r.v.denisenko@gmail.com, t.o.epifanova@gmail.com*

*Научный руководитель: канд. юрид. наук, доцент Ермакович С. Л.*

В рамках гражданского оборота участники правоотношений стремятся обеспечить защиту от недостоверных сведений с помощью системы распределения рисков. И чем сложнее становится конструкция договора, тем больше проявляется потребность в ней. Право Великобритании предусматривает такие институты, как «Warranties» (гарантии), «Representations» (заверения). Заверения представляют собой заявления о фактах, побуждающие заключить сделку. Гарантии – утверждения о фактах, которые будут действительными в будущем. Данные инструменты имеют огромное значение для участников гражданского оборота. Например, они позволяют продавцу заверить покупателя, что он имеет корпоративные полномочия совершать сделку или что корпорация действует в соответствии с законодательством своей страны.

До внесения соответствующих изменений в Гражданский кодекс Российской Федерации (далее – ГК РФ) российские юристы обращались к зарубежному опыту и использовали традиционные для английской правовой системы «Representations and Warranties». К сожалению, нормы российского права не позволяли применить санкции в случае предоставления недостоверной информации.

Статьи 178, 179 ГК РФ, предусматривающие признание сделки, совершенной под влиянием существенного заблуждения, обмана, насилия, угрозы или неблагоприятных обстоятельств, недействительной, практически не применялись, так как доказать факт введения в заблуждение, обман и т. д. –