

которого предполагается осуществление дипломатической защиты, в течение разумного срока после официального предъявления требования.

Государства, осуществляющие дипломатическую защиту в отношении бипатридов, зачастую руководствуются положениями двухсторонних соглашений. Однако это приводит к определенным сложностям в применении норм международного права к последующим ситуациям. Необходимым в таких ситуациях видится согласование рамочных соглашений о дипломатической защите бипатридов.

Жогло П. А.

К ВОПРОСУ ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ «КИБЕРПРЕСТУПЛЕНИЕ»

Жогло Полина Андреевна, учащаяся 3 курса Юридического колледжа Белорусского государственного университета, г. Минск, Беларусь, zhoglo.polly@mail.ru

Научный руководитель: преподаватель Головенчик М. Г.

Вследствие научно-технического прогресса возникает необходимость введения новых терминов, их определения, наделения их необходимыми признаками и т. д. Так, если термин подобран удачно, то он все больше используется в практическом обиходе, являясь понятным для многих слоев общества. Одним из таких терминов, стремительно и прочно вошедших в современный оборот, является «цифровизация».

В настоящее время термин «цифровизация» понимается в двух значениях – узком и широком. В узком смысле цифровизация представляет собой процесс или процедуру преобразования имеющейся информации в цифровую форму. Цифровизация в широком смысле является современным мировым трендом эффективного развития, пришедшим на смену компьютеризации, информатизации.

Технический прорыв, происходящий в той или иной области, с одной стороны, предлагает значительные перспективы в развитии общества, которые могут быть связаны с качественным изменением жизни. С другой стороны, известно, что изобретение, на первый взгляд, безобидных вещей может привести, например, к возникновению межгосударственных конфликтов.

На сегодняшний день угрозы, обусловленные широким распространением процесса цифровизации, объединены одним общим признаком – использованием информационно-коммуникационных технологий как способом совершения правонарушений в рассматриваемой сфере.

Западными учеными предложен специальный термин «*cybercrime*», что в переводе на русский язык означает киберпреступление. Но исследователями до настоящего времени так и не был выработан единый подход к пониманию понятия «киберпреступление». Так, в литературе было предпринято немало попыток дать общее понятие рассматриваемой группе преступлений:

«преступления в телекоммуникационных сетях», «компьютерные преступления», «преступления в сфере компьютерной информации», «преступление в СВТ» и др. Как отмечает белорусский ученый Н. О. Мороз, некоторые ученые используют понятия «киберпреступление», «компьютерное преступление», «преступление в СВТ» как синонимы. Полагаем, что прежде чем сформулировать определение понятия «киберпреступление», необходимо обозначить признаки рассматриваемой группы правонарушений.

По мнению российского ученого С. Ю. Бытко, одним из значимых признаков киберпреступлений является их совершение «online», или, иными словами, посредством использования специальных компьютерных или иных информационно-телекоммуникационных сетей. Данный признак характеризует обстановку совершения преступления.

Следующим признаком киберпреступлений называют их многообъектность, а основным непосредственным объектом рассматриваемых преступлений являются отношения, посредством которых обеспечивается информационная безопасность и защита от несанкционированного доступа в компьютерную сеть. Российский ученый Д. Ю. Гончаров отмечает, что в качестве факультативного объекта должны рассматриваться «связанные с ними общественные отношения», к которым могут быть причислены многие прочие объекты уголовно-правовой охраны.

В качестве самостоятельного признака киберпреступления выделяют особенности субъекта: лицо, обладающее специальными познаниями и навыками в работе с цифровой информацией, позволяющими модифицировать эту информацию таким образом, чтобы достичь поставленных преступных целей.

Рассматривая субъективную сторону данных преступлений, следует отметить, что их следует охарактеризовать как умышленные (совершенные с прямым или косвенным умыслом).

Отметим, что в литературе отмечают и иные свойства, которыми следовало бы наделять киберпреступления. В частности, к признакам киберпреступлений относят: трансграничность, тайность, продолжаемость, множественность мотивов. Данные признаки в большей степени применимы не для уголовно-правовой оценки содеянного, а для его криминологической характеристики и разработки криминалистических методик противодействия киберпреступности.

Таким образом, киберпреступление можно определить как умышленное противоправное деяние, совершаемое в локальной или глобальной компьютерной или иной информационно-телекоммуникационной сети, связанное с несанкционированным размещением, хранением, получением, модификацией 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.