

Таким образом, в рамках обеспечения общественной безопасности нарядами патрульно-постовой службы милиции общественной безопасности Министерства внутренних дел Республики Беларусь внедрение цифровых технологий предоставит возможность быстрой и своевременной передачи оперативно-дежурной службой территориального органа внутренних дел информации с места происшествия, что значительно повысит эффективность выбытия ближайшего наряда к месту происшествия, позволит быстро идентифицировать лиц и задержать виновных по горячим следам.

УДК 342.9

*П.В. Лутович*

## **МЕЖДУНАРОДНЫЙ ОПЫТ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ**

Киберпреступность создает серьезные проблемы для отдельных лиц, организаций и правительств во всем мире. Она охватывает широкий спектр преступных действий, которые осуществляются с использованием сети Интернет и других форм цифровых технологий. Анонимность сети Интернет затрудняет отслеживание и судебное преследование киберпреступников, а быстроразвивающийся характер технологий способствует появлению новых форм киберпреступности. Указанное обуславливает необходимость международного сотрудничества и развития правовой основы эффективной борьбы с киберпреступностью.

Изучение международного опыта правового регулирования противодействия киберпреступности может помочь в выявлении пробелов и несоответствий в национальном законодательстве, разработать более эффективные правовые меры противодействия киберпреступности.

Рассматриваемая проблематика нашла отражение в многочисленных трудах ученых, изучавших вопросы международного противодействия киберпреступности. Среди данных исследований можно выделить следующие основные направления: международные правовые и технические аспекты киберпреступности; международная реакция на киберпреступность и роль правоохранительных органов в борьбе с ней; политические и правовые аспекты международной киберпреступности; международная правовая база киберпреступности и проблемы, связанные с ней.

Анализ международных договоров, нормативных правовых актов и исследований в сфере правового регулирования киберпреступности позволяет заключить, что абсолютное большинство стран создали собственную правовую базу и имеют собственный подход к борьбе с киберпреступностью.

Так, в Великобритании действуют общие уголовные законы, которые могут применяться к киберпреступности. Закон о мошенничестве, например, предусматривает уголовную ответственность за мошенничество, в частности за мошенничество, связанное с компьютерной техникой. Закон о полномочиях на проведение расследований предоставляет властям необходимые полномочия для расследования киберпреступлений.

В Канаде действуют как специальные, так и общие законы по борьбе с киберпреступностью. Уголовный кодекс Канады предусматривает уголовную ответственность за взлом, кражу личных данных и другие преступления, связанные с компьютерной техникой. В стране также действуют такие законы, как Закон о защите личной информации и электронных документах, который непосредственно регламентирует защиту и конфиденциальность личных данных.

В ряде стран, таких как Китай и Иран, действуют законы, которые в большей степени направлены на цензуру и контроль над сетью Интернет, а не на киберпреступность как таковую. Закон о кибербезопасности Китая, например, предоставляет правительству широкие полномочия по контролю за онлайн-контентом, используется для судебного преследования лиц, осуществляющих киберпреступную деятельность, в том числе распространение ложной информации в сети Интернет.

В странах постсоветского пространства, в том числе в Республике Беларусь, законодательство в сфере противодействия киберпреступности все еще находится в стадии разработки, и в ряде случаев отсутствует специальное законодательство, в связи с чем правоприменители основываются на общем законодательстве.

В качестве одного из направлений совершенствования национального законодательства представляется возможным изучение опыта правового регулирования противодействия киберпреступности в Соединенных Штатах Америки, где разработано специальное законодательство, направленное на борьбу с киберпреступностью. Ключевыми законодательными актами в этой сфере являются:

Закон о компьютерном мошенничестве и злоупотреблениях – предусматривает уголовную ответственность за взлом и другие преступления, связанные с компьютерами; запрещает несанкционированный доступ к защищенным компьютерным системам и кражу информации из этих систем; предусматривает усиленные наказания для рецидивистов и тех, кто приводит к уничтожению или повреждению защищенных компьютерных систем;

Закон о конфиденциальности электронных коммуникаций – предусматривает защиту электронных коммуникаций и данных, хранящихся на электронных устройствах; запрещает несанкционированный доступ к электронным сообщениям и их перехват без судебного решения;

Закон о предотвращении кражи личных данных – устанавливает, что кража личных данных является федеральным преступлением; запрещает отдельным лицам умышленно передавать или использовать средства идентификации другого лица с намерением совершить незаконную деятельность;

«Патриотический акт» – расширяет полномочия правоохранительных органов по контролю за пользователями сети Интернет и телефонной сети; обязал крупнейших сетевых гигантов и сервис-провайдеров сотовой связи осуществлять контроль за отдельными лицами и организациями, подозреваемыми в причастности к киберпреступной деятельности;

Закон об обмене и защите киберразведки (поправка к Закону о национальной безопасности) – поощряет частные компании делиться информацией о киберугрозах с правительством, а также освобождает от ответственности компании, которые предоставляют такую информацию.

Среди ключевых направлений совершенствования международного противодействия киберпреступности необходимо выделить следующие:

расширение международного сотрудничества и координации рассматриваемой деятельности – заключение международных соглашений для облегчения обмена информацией и выдачи киберпреступников, создание международных организаций для содействия сотрудничеству между странами в борьбе с киберпреступностью;

гармонизацию законов и подзаконных актов разных стран – разработку международных стандартов защиты данных и создание общей правовой базы в сфере киберпреступности;

обучение и повышение квалификации сотрудников правоохранительных органов в сфере киберпреступности – обучение последним тенденциям в сфере противодействия киберпреступности;

развитие партнерских отношений между государством и частным сектором – повышение эффективности международного противодействия киберпреступности (обмен информацией и ресурсами между правоохранительными органами и частными компаниями, создание государственно-частных целевых групп для борьбы с киберпреступностью);

повышение способности правоохранительной системы обнаруживать и предотвращать киберпреступления до того, как они произойдут, – разработку передовых технологий, методов и способов выявления и отслеживания киберпреступников, внедрение мер безопасности;

проведение международных исследований в области киберпреступности – лучшее понимание проблемы и разработку эффективных стратегий для ее решения.

В заключение следует отметить, что правовое регулирование противодействия киберпреступности отличается в разных странах, что необходимо учитывать при организации эффективного международного сотрудничества. По нашему мнению, совершенствование рассматриваемой деятельности требует координации, гармонизации законов и подзаконных актов, профессиональной подготовки специалистов, развития государственно-частного партнерства, технологий, методов и способов выявления киберпреступников и проведения научных исследований.

УДК 343.211

**А.А. Матчанов**

### **ЗНАЧЕНИЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ГОСУДАРСТВ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ**

Республика Узбекистан целенаправленно осуществляет политику непримиримой борьбы с преступностью и осуществления эффективного международного сотрудничества государств в данной сфере. Двусторонние и многосторонние, универсальные и региональные международные договоры и соглашения регулируют и систематизируют международное сотрудничество в борьбе с преступностью. Основываясь на ратифицированных международных нормах, аналогичную функцию выполняют национальные законодательные акты.

В современный период преступность все больше приобретает транснациональный характер и представляет международную угрозу нормальному функционированию государственных и общественных институтов. Государство, являясь главной организующей силой гражданского общества, определяет основные, приоритетные задачи в этой области посредством создания соответствующих правоохранительных структур, в числе которых особо важное место занимают органы внутренних дел. Однако с этой проблемой, приобретающей международный характер, отдельной стране в одиночку не справиться. Решение данной проблемы видится в совершенствовании механизма международного сотрудничества правоохранительных органов государств, их совместных действий в борьбе с преступностью. Это в полной мере относится к Узбекистану как полноправному члену мирового сообщества. Сегодня перед нашей страной стоят реальные угрозы, связанные с организованной, транснациональной, киберпреступностью, торговлей людьми, коррупцией, наркотрафиком и др. Необходимость противодействия этим угрозам требует эффективного и адекватного ответа, обеспечения четких и слаженных действий всех подразделений правоохранительных органов государств.

Следует отметить, что международное сотрудничество имеет комплексный, многоотраслевой характер, предусматривает необходимость имплементации международных норм в национальное законодательство страны. Кроме того, оно предусматривает координацию деятельности соответствующих правоохранительных органов государств, а также соответствующих международных организаций в обеспечении прав человека в борьбе с преступностью. При этом нормативно-правовые взаимоотношения международных организаций и внутригосударственных структур предусматривают непосредственное взаимодействие правоохранительных органов государств между собой.

Интерпол тесно сотрудничает с национальными правоохранительными органами, входя в их структуру как национальные центральные бюро Интерпола. Наряду с ними имеются другие международные организации и национальные государственные структуры, деятельность которых в целом направлена на разрешение иных задач, но при их выполнении имеются аспекты, которые затрагивают проблемы борьбы с преступлениями и обеспечения прав человека в правоприменительной деятельности страны.