

**Боталов Н. М.**

## **ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ АНОНИМНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА УРОВНЕ СОЮЗНОГО ГОСУДАРСТВА БЕЛАРУСИ И РОССИИ**

*Боталов Никита Михайлович, студент 3 курса МИРЭА – Российского технологического университета, г. Москва, Россия, botalov.n.m@mail.ru*

*Научный руководитель: канд. юрид. наук, доцент Смирнов М. Г.*

Преступления, совершаемые с использованием анонимных телекоммуникационных сетей, таких как «DarkNet», отличаются специфическими особенностями. Эти сети предоставляют высокий уровень анонимности, что затрудняет идентификацию преступников и делает данные преступления сложно расследуемыми.

«DarkNet» представляет скрытую часть интернета, которая недоступна через стандартные поисковые системы и требует специальных программ для доступа, таких как Tor или I2P. Хотя сеть «DarkNet» может использоваться для легитимных целей, например, для защиты приватности, она также связана с незаконной деятельностью, что делает ее потенциально опасной.

«DarkNet» де-факто является площадкой для торговли нелегальными товарами, такими как наркотики, оружие, поддельные документы, а также для организации хакерских атак и распространения вредоносного программного обеспечения, часто используется для отмывания денег и финансовых махинаций, где криптовалюты, такие как Bitcoin, играют центральную роль. В «темном интернете» активно работают хакерские группы, которые могут атаковать различную инфраструктуру, в том числе и государственную.

В свою очередь, в России, по данным Роскомнадзора, число преступлений, связанных с распространением наркотиков через интернет, выросло на 30–40 % за последние несколько лет. По данным Министерства внутренних дел Республики Беларусь, число преступлений, связанных с наркотиками и совершенных с использованием анонимных телекоммуникационных сетей, выросло на 40 % за последние пять лет.

Анонимные сети в СНГ используются также для распространения экстремистских идей и вербовки сторонников для террористических организаций. Россия и Центральная Азия (Казахстан, Таджикистан, Узбекистан) особенно подвержены этой угрозе. С 2016 г. наблюдается активное использование «DarkNet» для распространения материалов, связанных с экстремистскими группировками, в том числе с ИГИЛ.

В рамках Союзного государства Беларуси и России сотрудничество в вопросах кибербезопасности и противодействия киберпреступности приобретает особую актуальность. Россия и Беларусь совместно развивают программы по мониторингу активности в «DarkNet» с целью выявления потенциальных угроз для национальной безопасности. Созданы совместные центры кибербезопасности, которые координируют действия в случае

выявления угроз. Одним из таких примеров является сотрудничество между российским Национальным координационным центром по компьютерным инцидентам (НКЦКИ), уполномоченным осуществлять внутрироссийское и международное взаимодействие по вопросам реагирования на компьютерные инциденты, в которые вовлечены российские информационные ресурсы, и белорусскими спецслужбами.

Стоит отметить прошедшие в сентябре 2023 г. российско-белорусские учения «Щит Союза», в рамках которых были рассмотрены сценарии кибератак и проведение мероприятий по противодействию таковым. Однако в связи с ростом подобных преступлений этих усилий может быть недостаточно.

Предполагается, что создание единого правового поля в сфере противодействия киберпреступлениям будет способствовать повышению эффективности расследований в данной области, в том числе имеет под собой значимый посыл и создание единого цифрового пространства между союзными государствами, что позволит унифицировать политику в сфере противодействия нарушениям в цифровом поле и киберсфере.

Таким же образом стоит создать единую сеть мониторинга и противодействия киберугрозам, акцентируя внимание на преступности, связанной с использованием анонимных телекоммуникационных сетей, для создания лучших условий противодействия подобного рода преступлениям.

Предлагаем закрепить сотрудничество в данной сфере на уровне межправительственного договора, который бы регламентировал полномочия и порядок осуществления подобной деятельности между союзными государствами. Подобный проект может включать в себя положения о создании межгосударственного органа, в полномочия которого будет включаться обеспечение единой политики в цифровом пространстве, а также возможность вести расследования и унифицировать подходы к таковому между двумя странами.

***Бухов Г. И.***

## **ПРЕДДоговорный этап заключения договора предоставления безвозмездной (спонсорской) помощи**

*Бухов Георгий Игоревич, магистрант юридического факультета  
Белорусского государственного университета, г. Минск, Беларусь,  
buhovgeorgii@gmail.com*

*Научный руководитель: канд. юрид. наук, доцент Свадковская Е. А.*

Последовательность формирования договорных отношений связана с комплексом факторов, ее предопределяющих. Одним из предопределяющих факторов является экономическая цель заключения договора, впоследствии обуславливающая избрание конкретного вида договорного обязательства. В ряде случаев одна цель может быть достигнута через заключение различных типов (видов) гражданско-правовых договоров, в других же – это возможно с использованием одного конкретного из них. Остановимся