отношении которых имеется более всего доказательств, дальше допрашиваются те лица, которые могут сообщить больше важной информации по обстоятельствам того, что произошло.

Таким образом, наиболее эффективным следственным действием относительно получения информации является допрос как основное следственное действие, которое проводится на первоначальном этапе расследования преступлений, связанных с нарушением прав потребителей.

Список использованных источников

1. О защите прав потребителей: Закон Донецкой Народной Республики от 05.06.2015 № 53-IНС, действующая редакция по состоянию на 16.03.2020 // Официальный сайт Народного Совета Донецкой Народной Республики. – URL: dnrsovet.su/zakon-dnr-o-zashhite-prav-potrebitelej/. – Текст: электронный.

2. Панов, Н., Шепитько, В. Рефлексивное управление при допросе // Юридический вестник. – 1999. – № 4. – С. 96-98. – Текст: непосредственный.

3. Шепитько, В.Ю. Справочник следователя. – Киев: Издательский Дом «Ин Юре», 2001. – 216 с. (Серия «Библиотека следователя»). – Текст: непосредственный.

4. Коновалова, В.Е. Допрос: тактика и психология. – Харьков: Консум, 1999. – 157 с. – Текст: непосредственный.

ЦИФРОВОЕ ГОСУДАРСТВО: КРИМИНОЛОГИЧЕСКИЙ И УГОЛОВНО-ПРАВОВОЙ АСПЕКТЫ

Боровик А.А.,
Донецкая академия внутренних дел
Министерства внутренних дел
Донецкой Народной Республики
Шпатусько Ю.П.,
Донецкая академия внутренних дел
Министерства внутренних дел
Донецкой Народной Республики

Необходимость рассмотрения данной темы обусловлена тем, что развитие и проникновение информационных технологий в общество носит тотальный характер на сегодняшний день. Внедрение цифровых технологий в социум имеет как позитивные, так и негативные последствия, так как благодаря данному

инструменту появилось огромное количество способов воздействия на человека и общество в целом. Также к негативным последствиям можно отнести появление новой формы преступности – преступность в сети Интернет, социальных сетях (киберпреступность). В этом случае, компьютерные сети выступают в качестве объекта преступных посягательств, а также средства или способа совершения преступлений [4, с. 45].

Итак, уже на протяжении десятилетия борьба с цифровой преступностью находится во внимании цивилизованных стран всего мира. Однако постоянное развитие и совершенствование информационных технологий являются благоприятными условиями для увеличения количества киберпреступников и для угрозы не только глобальных информационных сетей, но и всего общества [5, с. 29]. Проблема киберпреступности состоит в том, что выделить способы противодействия данному виду преступления невозможно, так как преступники с легкостью приспосабливаются к новым мерам безопасности. Невозможно не согласиться с мнением А.В. Манойло, что преступников привлекают возможности самого Интернета, социальных сетей: во-первых, открыт доступ к банковским и финансовым платежным системам, системам хранения конфиденциальной информации и т.д.; во-вторых, в Интернете предоставляется возможность действовать анонимно, а также с легкостью можно уничтожить улики, например, удалить переписку, либо же вовсе не оставить следов преступления, с помощью прокси-сервера [3].

Все дошло до того, что рассмотрение социальных сетей в качестве орудия преступления в юридической литературе стало нормой. Криминализации информационного пространства в социальных сетях особое внимание начали уделять в 2015-2017 гг., когда с помощью групп «ВКонтакте» подростков подстрекали на суицид в онлайн-режиме [2]. Представителям правоохранительных органов долгое время не удавалось выявить подстрекателя, как раз благодаря анонимности сайта и возможности указывать лживые (выдуманные) личные данные, а также из-за отсутствия специальных знаний и навыков у сотрудников правоохранительных органов в сфере информационных технологий.

Кроме того, в сети Интернет активно процветает мошенничество, предоставляется возможность для махинации со счетами, злоумышленники взламывали сайты, которые активно используют в своей деятельности бухгалтеры, а также сайты популярных СМИ и крупных магазинов и заражали их вредоносными программами Win32/Carberp и Win32/ Rdpdor. Установив при этом скрытный удаленный доступ к компьютеру потенциальной жертвы и обнаружив на нем программы и реквизиты для работы с банковскими счетами,

«заливщики» формировали мошенническое платежное поручение о перечислении денежных средств на заранее подготовленный счет, после чего похищенные деньги обналичивались посредством банковских карт, оформленных на подставных физических или юридических лиц, «обнальщиками», отвечавшими за организацию работы «дропов» («мулов») – лиц, непосредственно открывавших банковские счета или платежные карты, на которые переводились похищенные денежные средства, и впоследствии снимавших похищенные денежные средства для последующей их передачи «обнальщику» [1, с. 101]. Таким образом, Интернет является отличным способом для легализации денежных средств, полученных преступным путем.

Как уже было сказано, способы противодействия киберпреступности необходимо регулярно совершенствовать, так как хакеры быстро ко всему приспосабливаются. Единственный способ искоренить преступления в сети – это отключение сети Интернет во всем государстве, однако это невозможно.

Итак, для борьбы с преступностью в глобальных информационных сетях сотрудники правоохранительных органов должны получать специальные знания и опыт. Следующим шагом для борьбы с данным видом преступления, может стать разработка международной правовой базы. Так как Интернет представляет собой открытую среду, дающую пользователям возможность совершать определенные действия за пределами границ государства, в котором они находятся, необходимо наладить международное сотрудничество, так как оказывать противодействие киберпреступности на территории отдельного государства невозможно. Международное сотрудничество является ключевым моментом для сдерживания такого комплексного явления, как киберпреступность. Совместная работа государств и международных организаций, выработка новых механизмов контроля и управления – единственный путь к информационной безопасности, которая в настоящее время представляется труднодостижимой целью, но в то же время является насущной необходимостью.

Список использованных источников

1. Бегишев, И.Р., Хисамова, З.И., Никитин, С.Г. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты // Всероссийский криминологический журнал. – 2020. – № 1. – С. 96-105. – Текст: непосредственный.

2. Гончарова, А.А. Преступность в социальных сетях как фактор угрозы духовному развитию молодежи / Сайт: Radnews. – URL:

http://www.radnews.ru/преступность-в-социальных-сетях-как-ф/. – Текст: электронный.

3. Манойло, А.В. Криминализация информационного пространства и преступная деятельность экстремистских группировок в социальных сетях // Сайт: Межрегиональное бюро судебных экспертиз имени Сикорского. – URL: https://www.expertsud.ru/content/view/207/36/. – Текст: электронный.

4. Номоконов, В.А., Тропина, Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 1(24). – С. 45. – Текст: непосредственный.

5. Протасевич, А.А., Зверянская, Л.П. Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – № 3. – С. 28-33. – Текст: непосредственный.

ОСНОВАНИЯ И УСЛОВИЯ ДОПУСКА ПЕРЕВОДЧИКА К УЧАСТИЮ В СУДОПРОИЗВОДСТВЕ

Катаев Е.В.,
Донецкая академия внутренних дел
Министерства внутренних дел
Донецкой Народной Республики

Привлечение переводчика в судопроизводство в реалиях многонационального государства является довольно распространенным явлением. В связи с этим правильное процессуальное оформление привлечения является гарантией того, что оснований для обжалования у стороны защиты не будет.

Необходимость анализа оснований и условий допуска переводчика к участию в судопроизводстве обусловлена наличием большого числа связанных с этим процессуальных и организационных проблем. В научной литературе отмечается распространенность таких нарушений, как привлечение недостаточно компетентного переводчика; несвоевременное привлечение переводчика; отказ дознавателя в привлечении переводчика в случаях, когда его помощь в действительности нужна; нарушение процедуры привлечения переводчика (отсутствие постановления, неразъяснение ответственности переводчику) и др. Нарушения, допущенные в ходе проведения предварительного следствия и дознания являются основанием для признания