уровне никак нельзя разработать и закрепить процедуру или процесс заботы, бережного отношения, уважения и многое другое.

Следует отметить, что приведенные выше основания для классификации конституционных обязанностей граждан в различные взаимосвязанные группы не являются исчерпывающими. Например Кендзя З., исследуя возможные варианты классификации основных обязанностей граждан, использует попытки классифицировать обязанности граждан в соответствии со сферами жизни, которых касаются эти обязанности, им выделяются: а) обязанности граждан перед государством общего характера, б) обязанности граждан в области обороноспособности, в) обязанности граждан в области экономики.[5]

Таким образом, перечень оснований для классификации конституционных обязанностей граждан весьма широк. Каждая из приведенных выше классификаций имеет свои плюсы и минусы и может быть применена при изучении тех или иных свойств конституционных обязанностей. Однако разнообразие классификаций ни в коем случае не свидетельствует об обособленности отдельных групп обязанностей друг от друга. Каждая из названных классификаций предполагает взаимосвязь существующих в ней групп. Выделение же тех или иных групп обязанностей граждан лишь помогает более глубоко познать их сущность посредством отдельного изучения, анализа разрозненных групп.

Список литературы:

1. Конституция Республики Казахстан // Ведомости Парламента Республики Казахстан, 1996 г., N 4, ст. 217 с изм. и доп. от 23.03.2019 г./ http://adilet.zan.kz/

2. Андреева Г.Н. Конституционное право зарубежных стран: Учебник. – М.: Изд-во Эксмо, 2005. – 656 с.

3. Барзилова Ю.В. Юридические обязанности как элемент правового статуса личности: дисс. канд. юрид. наук. – Саратов, 2006. – 199 с.

4. Витрук Н.В. Основы теории правового положения личности в социалистическом обществе. – Москва: Наука, 1979. – 229 с.

5. Коршунова И.В. Обязанность как правовая категория: Автореф. дисс. канд. юрид. наук. – Москва, 2004. – 27 с.

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Мертимиров А.,
магистрант первого курса кафедры уголовного процесса и криминалистики
КарУ им. Е.А.Букетова

Происходящие преобразования в современных обществах и государствах, когда мир находится в условиях карантина, связанного с пандемией COVID-19, объявленной Всемирной организацией здравоохранения в марте 2020 года, онлайн формат деятельности, цифровизация, развитие информационно-коммуникационных технологий (ИКТ) активизировали рост киберпреступлений во всем мире. Цифровизация и стремительное развитие и внедрение новейших информационно-коммуникационных технологий предоставляют широкие возможности для интеграции научных знаний, участия в общественно-политической и социальной

жизни, доступа к финансово-экономическим перспективам, образовательному процессу, быстрому обмену информацией и общению вне зависимости от территориального расположения.

Однако указанные факторы научно-технического прогресса имеют и свою теневую сторону, которая выражается в возникновении нового криминалистического вида преступлений, совершаемых в киберпространестве, то есть в альтернативной реальности, отличной от живого общения. Возможности информационно-коммуникационных технологий характеризуются в первую очередь, быстротой передачи информации, появления новых финансовых продуктов, что является предпосылками для их неправомерного использования, в целях совершения антисоциальных, агрессивных криминальных действий. Такого рода антисоциальные, аморальные и агрессивные действия в киберпространстве приобретают характер киберпреступлений, которые выражаются в различных видах преступлений, начиная от подстрекательства к суициду, сексуальной эксплуатации, мошеннических действий и заканчивая провокацией массовых беспорядков, провокации к террористической и экстремистской деятельности.

Необходимо отметить, что в своей основе киберпреступления всегда имеют проявления агрессивного поведения латентного характера, и именно в киберпространстве в полной мере выражаются различные формы агрессии и выражения расстройств поведения, направленных против отдельных лиц, групп людей и/или целевых групп населения, с целью причинения вреда последним.

В настоящее время, наиболее распространенными киберпреступлениями являются такие их виды, как сексуальная эксплуатация детей и сексуальное надругательство над детьми в сети Интернет, киберпреследование, кибердомогательство, кибертравля, различные формы криминальных деяний на гендерной почве (например, сексуальное вымогательство), а также киберпреступления, террористической и экстремистской направленности.

Указанное не только актуализирует разработку мер противодействия киберпреступлениям, и их предупреждению, но и тщательного научного анализа и оценки криминальных деяний в киберпространстве, что уже наделяет их специфическими особенностями криминалистической характеристики и процесса расследования в целом.

Как указывалось ранее, наиболее опасными являются киберпреступления против личности, тенденция быстрого роста, которых отмечается не только в Казахстане, но и на территории стран СНГ.

По нашему мнению, особенностью киберпреступлений является определение основных элементов их криминалистической характеристики, что обуславливает в конечном счете особенности их расследования.

Исходя из указанного определения киберпреступлений, ведущими, доминирующими элементами криминалистической характеристики рассматриваемого криминалистического вида преступлений является взаимосвязь преступника и его жертвы, а также обстановка их совершения, что и определяет специфические особенности расследования.

Киберпреступления против личности могут совершаться одним или несколькими преступниками в отношении одной или нескольких жертв и\их близких в любой точке мира, где есть подключение к сети Internet, что весьма затрудняет задачу контроля правоохранительными органами за такими преступлениями [1, с.565]

Киберпреступления против личности могут иметь значительные неблагоприятные социальные, экономические и психологические последствия для жертв киберпреступлений, включая расстройства поведения вызванные негативными эмоциональными состояниями

(страх, тревога, депрессия, стыд как моральное страдание, утрата социального статуса и человеческого достоинства, репутационный вред, финансовые затраты, связанные с медицинскими и консультационными услугами, юридической помощью, а также услугами по защите данных в Интернете, программным обеспечением и мерами обеспечения безопасности в офлайновой среде, суицид) [2]

В этой связи, киберпреступления требуют особого внимания, с позиций тяжести последствий, в том числе необратимого характера.

Как правило, преступником и жертвой киберпреступлений, могут быть люди различных возрастных групп, половой, расовой, этнической принадлежности, сексуальной ориентации, социального, религиозного и культурного статуса, семейного положения.

При этом, в рассматриваемом криминалистическом виде преступлений, могут быть и исключения, которые находятся в зависимости от субъекта и объекта преступного посягательства (например, жертвами сексуальной эксплуатации детей и сексуального насилия над детьми являются дети)

Киберпреступления предполагают использование информационно-коммуникационных технологий в качестве средств для совершения различных видов преступлений.

Например, сексуальная эксплуатация несовершеннолетних и сексуальное насилие над несовершеннолетними в сети Internet запрещены международным и национальным законодательством Республики Казахстан и представляют собой серьезную форму насилия.

Необходимо отметить, что киберпреступления против личности имеют различные проявления, в том числе груминг, размещение материалов с изображением сексуального насилия над детьми/материалов с изображением сексуальной эксплуатации детей и прямая трансляция сексуального насилия над детьми.

Киберпреступления в форме груминга в типичных случаях происходит поэтапно, начиная с этапа выбора жертвы в сети Internet. Это связано с тем, что дети являются участниками различных социальных сетей и коммуникационных приложений, которые преступники могут использовать для получения доступа к учетным записям детей.

Необходимо подчеркнуть, что механизм совершения киберпреступлений начинается с активного поиска жертвы преступления. Как правило, выбор жертвы преступления основывается на основании психологических характеристик, а именно:

– привлекательность-притягательности жертвы для преступника;

– легкости доступа в информационно-коммуникационных сетях (например, в зависимости от используемых несовершеннолетними настроек безопасности на веб-сайтах, платформах, приложениях);

– степени уязвимости жертвы (например, сообщение о своем одиночестве или чувстве непонимания)

Как правило, после выбора жертвы преступник связывается с последней, с целью получить доступ и вступить с ней в определенные, выгодные отношения, используя при этом установленную уязвимость жертвы, отсутствие реального, живого контакта, возможности скрывать свою личность (что фактически определяет совершение киберпреступлений в идеальных условиях, в условиях неочевидности)

Кроме того, подготовка к совершению всех киберпреступлений, в том числе против личности является для преступника процессом, не требующим привлечения значительных ресурсов и средств, при этом минимизирует возможность оставить следы преступной деятельности.

Подготовка к совершению всех киберпреступлений основывается на сборе и использовании в преступных целях, информации из легальных источниках о жертве, так как личные данные указываются самой жертвой преступлений в сети.

Цель киберпреступника заключается в дальнейшем развитии отношений в киберпространстве, которое не обеспечено в достаточной степени правовой безопасностью (например, блогчейн), что ведет к значительному повышению рисков совершения различных видов киберпреступлений.

Необходимо отметить, что особенностью совершения различных видов киберпреступлений является тщательная оценка преступником рисков, связанных с его обнаружением и установлением. Это обуславливает достаточно продуманное поведение преступника по сокрытию виртуальных следов (например, использование чужого IP-адреса, систему теневого интернета и пр.), а также психологических приемов влияния на жертву (например, сообщает об исключительности их отношений и необходимости держать эти отношения в тайне и пр.)

Процесс совершения киберпреступлений является это динамическим процессом, в основе которого лежат мотивация и возможности преступника, а также способность преступника манипулировать жертвой и контролировать ее.

Преступный результат киберпреступлений это различные формы насилия над жертвой в сети Internet (например, путем манипулирования или склонения жертвы к передаче денежных средств, участия в военных действиях, снятие фото или видео сексуального характера и отправке его преступнику)

Киберпреследование, как форма киберпреступлений предполагает использование информационно-коммуникационных технологий для совершения неоднократных действий с целью домогательства, беспокойства, нападок, угроз, запугивания и/или словесного оскорбления отдельных лиц на систематической основе для достижения целей преступника

Преступники могут осуществлять киберпреследование напрямую посредством электронной почты, мгновенных сообщений, звонков, текстовых сообщений или иных форм электронной коммуникации для передачи непристойных, вульгарных и/или оскорбляющих достоинство высказываний и/или угроз жертве и/или семье, партнерам и друзьям жертвы, и использовать технологии для мониторинга, наблюдения и отслеживания передвижений жертвы (например, путем тайной установки устройств GPS-слежения в автомобили, сумки и даже детские игрушки и пр.)

Кроме того, киберпреследование может осуществляться косвенным путем посредством причинения ущерба цифровому устройству жертвы (например, путем заражения компьютера жертвы вредоносной программой и использования этой программы для тайного мониторинга за жертвой и/или кражи информации о жертве) или размещения ложной, порочащей или оскорбительной информации о жертве в Internet, или создания поддельной учетной записи на имя жертвы для размещения материалов в Internet (социальных сетях, чатах, дискуссионных форумах, веб-сайтах и т. д.).

Киберпреследование подразумевает серию поступков и действий в течение некоторого периода времени, цель которых заключается в том, чтобы запугать, встревожить, устрашить или домогаться жертвы и/или семьи, партнера и друзей жертвы.

Указанное носит характер психологического насилия, и включают в себя такие действия, как: заполнение почтового ящика пользователя электронными письмами; частые размещение сообщений на сайтах, страницах и учетных записях пользователя в социальных сетях; многократные звонки и/или отправка текстовых сообщений жертве; оставление голосовых сообщений и отправка запросов на подписку и добавление в друзья; присоединение ко всем

группам и сообществам в сети, участником которых является жертва, или подписка на публикации жертвы через учетные записи знакомых, коллег, одноклассников, членов семьи или друзей в социальных сетях; и непрерывный просмотр страницы жертвы (некоторые вебсайты регистрируют эту информацию и сообщают пользователю, когда его страница просматривается).

Кибердомогательство предполагает использование информационно-коммуникационных технологий для преднамеренных действий с целью унижения, раздражения, нападок, угроз, запугивания, нанесения обиды и/или оскорбления.

Для признания факта совершения киберпреступления достаточно одного лишь инцидента; однако такое киберпреступление может включать в себя несколько инцидентов.

Кроме того, кибердомогательство может также предполагать целенаправленное домогательство, когда один или несколько человек объединяют усилия для многократного домогательства к своей жертве в Интернете в течение ограниченного периода времени с целью, причинения моральных страданий жертве, путем унижения и в конечном счете принудить жертву к действиям выгодным для преступника.

Кибердомогательство может также предполагать размещение или распространение иным способом ложной информации или слухов о человеке, чтобы причинить ущерб его социальному положению, межличностным отношениям и/или репутации. Такого рода ложная информация размещается на веб-сайтах, в чатах, мессендерах социальных сетей, форумах, социальных сетях и прочих Internet сайтах, чтобы опорочить репутацию жертвы.

Преступники могут также выдавать себя за жертв путем создания учетных записей со схожими именами, размещая на них существующие фотографии жертв, и использовать эти учетные записи для отправки запросов на добавление в друзья и/или подписку друзьям и членам семьи жертв, чтобы обманным путем вынудить их принять эти запросы (так называемая форма персонации в киберпространстве).

Принятие этих запросов в социальных сетях, обеспечивает преступникам доступ к учетным записям окружения жертвы, и, следовательно, доступ к реальным учетным записям жертв.

Необходимо отметить, что развитие и совершенствование информационно-коммуникационных технологий, создают условия для совершения киберпреступлений, террористической и экстремистской направленности, в сфере противодействия легализации незаконных доходов и финансирования терроризма.

Радикальная деятельность таких киберпреступных групп/сообществ, осуществляется в социальных сетях, и направлена на нанесение вреда психическому, физическому здоровью человека, лишения жизни, что собственно определяет их, как дистанционный способ совершения преступлений насильственного характера, посредством виртуального пространства сети интернет.

По нашему мнению, рассматриваемые сообщества, образуют, социальные группы, находящиеся во взаимодействии с социальным миром, посредством обмена информацией. Эти объективные условия информационного обмена между отдельной личностью, социальными группами/сообществами, нацелены на построение межличностных отношений и определенное сотрудничество. При этом начинает формироваться иерархия в сообществе, где на определенном этапе появляется криминальная личность в качестве организатора виртуальной группы/сообщества, который начинает диктовать условия для дальнейшего пребывания потенциальной жертвы в образовавшейся виртуальной группе.

По нашему мнению, между организатором преступлений и его потенциальными жертвами устанавливается психологический контакт, влияние на жертв в виде определения совместных целей и достижения общих интересов с виртуальной группой. Конечная цель в данном случае это принуждение к общению, основанном на шантаже и страхе (например, убеждение в совершении акта суицида, и пр.) Мотивом в этом случае выступает демонстрация личной власти над более слабой личностью, достижение ощущения собственной уникальности, важности, проявление собственной воли в реализации интересов и достижении поставленных целей, чувство безнаказанности и возможности анонимности в общении, что облегчает проявление внутренних патологических потребностей. Объективная составляющая формирования рассматриваемых виртуальных групп это резкое снижение морально-нравственных ценностей, отсутствие должного воспитательного процесса со стороны родителей, недостаточная общественно-полезная, интеллектуальная и творческая занятость. В качестве сохранения социального благополучия и не допущения социальной дестабилизации в обществе, особое значение, приобретает укрепление воспитательных мер, идеологических начал и информационной безопасности, как приоритетная форма противодействия экстремистским формам психологического давления в молодежной среде, как современного Казахстана так и сопредельных государств и обществ. Доминирующим фактором в противодействии деятельности рассматриваемых криминальных групп это обеспечение информационно-медийной безопасности общества, т.к. криминальные действия осуществляются посредством виртуального пространства, т.е. дистанционно, и следовательно имеет специфическую особенность быстрого распространения.

Таким образом, на основе нарушения информационно-медийной безопасности могут распространяться экстремистские идеи суицидального и иного деструктивного характера, а также формироваться криминальное поведение социальных групп. В данном случае криминальное поведение образует деятельность, направленную дистанционное убийство, в том числе несовершеннолетних, молодежь, реально и потенциально наносит существенный вред общественному сознанию, психическому и физическому здоровью, и государственным устоям в целом.

Список литературы

1. Henry, Nicola, Flynn, Asher and Powell, Anastasia. (2018). Policing Image-based Sexual Abuse: Stakeholder Perspectives. *Police Practice and Research: An International Journal*, Vol. 19(6), 565-581.

2. УНП ООН (2015). Исследование влияния новых информационных технологий на совершение надругательств над детьми и их эксплуатацию. https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.