Третью группу механогомических следов будут составлять предметы, постоянно используемые человеком: трости, опорные палки, костыли, очки, слуховые аппараты.

Еще одну группу могут составлять личные вещи человека, отражающие склонности и вкусы того, кто ими пользуется: авторучки, зажигалки, брелоки, запонки, броши, носовые платки, ремни, бумажники и другие. На наш взгляд, как отдельную группу можно рассматривать следы примененных косметических средств (губной помады, лака, румян, парфюма и т. п.),

Заключение. Таким образом, следы, оставленные на месте преступления, являются одним из основных источников информации, поскольку они содержат в себе такие сведения, которые нельзя получить из других каналов. Объективный характер такой информации связан с материальной природой следов. Поэтому механогомические следы открывают короткий путь к установлению лица, совершившего преступление.

1. Слесарева, П.А. Механогомические следы человека: определение понятия и место в классификации / П.А. Слесарева // XIII Машеровские чтения: материалы междунар. науч.-практ. конф. студентов, аспирантов и молодых ученых, Витебск, 18 октября 2019 г. / редкол.: И.М. Прищепа (гл. ред.) [и др.]. – Витебск: ВГУ имени П.М. Машерова, 2019. – С.398–400.
2. Грановский, Г.Л. Основы трасологии 2-е изд. / Г.Л. Грановский. – М, 2006. – 452 с.
3. Крылов, И.Ф. Криминалистическое учение о следах / И.Ф. Крылов. - Л., 2009. – 245 с.
4. Литвиненко, Л.К. Понятие и классификация следов в трасологии / Л.К. Литвиненко. – Киев, 2001. – 224 с.
5. Пророков, И.И. Криминалистическая экспертиза следов / И.И. Пророков. - Волгоград, 1980. – 286 с.
6. Шевченко, Б.И. Теоретические основы трасологической идентификации в криминалистике / Б.И. Шевченко. – М., 1995. – 96 с.
7. Якимов, И.Н. Практическое руководство к расследованию преступлений / И.Н. Якимов. – М., 1924. – 210 с.
8. Батычко, В.Т. Криминалистика в вопросах и ответах / В.Т. Батычко. - Таганрог: ТТИ ЮФУ, 2009. – 460 с.

О ПОНЯТИИ «КИБЕРПРЕСТУПНОСТЬ»

Таганов С.А.,
студент 4 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Стаценко В.Г., канд. ист. наук, доцент

Развитие информационно-коммуникационных технологий породило целый ряд новых проблем преступности, которых не существовало еще несколько десятилетия назад. Одной из таких проблем стала т.н. киберпреступность, которая представляет собой в настоящее время нарастающий вызов, как для общества в целом, так и для права и криминологического знания. Как отмечалось в Сальвадорской декларации 2010 года «О комплексных стратегиях для ответа на глобальные вызовы», принятой Резолюцией 65/230 Генеральной Ассамблеи, «развитие информационно-коммуникационных технологий и расширение масштабов использования Интернета создают новые возможности для преступников и способствуют росту преступности»… требуя «всестороннего исследования проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора, включая обмен информацией о национальном законодательстве, наилучших видах практики, технической помощи и международном сотрудничестве, с целью изучения возможных путей укрепления существующих и выработки предложений в отношении новых национальных и международных правовых или других мер по противодействию киберпреступности» [1].

В 2018 году исследование Центра стратегических и международных исследований (CSIS) показало, что ежегодно киберпреступность наносит ущерб около 600 миллиардов долларов, что составляет почти один процент мирового ВВП, а к 2022 году общий планетарный ущерб от киберпреступлений может достичь 8 триллионов долларов [2], что еще раз подчеркивает актуальность рассматриваемой проблемы.

Целью работы является рассмотрение содержания понятия «киберпреступность» в условиях отсутствия общепринятых и нормативно закрепленных соответствующих дефиниций.

Материал и методы. В работе использованы международно-правовые акты и нормативно-правовые акты Республики Беларусь, а также публикации зарубежных и отечественных исследователей. Работа выполнена на основе сравнительно-правового (компаративистского) метода, анализа документов.

Результаты и их обсуждение. Киберпреступность – это термин, широко используемый для описания деятельности, в которой компьютеры или компьютерные сети являются инструментом, целью или местом преступной деятельности. Киберпреступность принимает различные формы, включая кражу личных данных, кибersталкинг и другие формы интернет-мошенничества, нарушение авторских прав, хакерство, компьютерные вирусы, спам и пр. Многие виды киберпреступности являются развитием традиционной преступной деятельности, когда компьютер и интернет обеспечивают анонимность и защиту от правоохранительных органов.

В правовой и криминологической литературе понятие «киберпреступность» используется содержательно неоднозначно, причем, зачастую, в качестве синонимического используется термин «компьютерная преступность». В национальном праве термин «киберпреступность» практически не применяется, чаще в законодательстве различных стран употребляются понятия «компьютерные преступления», «информационные технологии», «преступность в сфере высоких технологий», «преступления в сфере компьютерной информации» и т.п. Например, раздел XII Уголовного кодекса Республики Беларусь «Преступления против информационной безопасно-

сти» включает в себя 7 статей, в наименовании и содержании которых превалируют понятия «компьютер», «компьютерная» (информация, система и т.п.) [3, ст. 34–355].

Немногие международно-правовые акты, в которых содержится понятие «киберпреступность», содержательно его не раскрывают.

Анализ международного законодательства и криминологической литературы, посвященной рассматриваемой проблематике, дает основание сделать вывод о том, что понятия «киберпреступность» и «компьютерная преступность», все же, содержательно отличаются. Термин «киберпреступность» более широко и точно отражает всю совокупность преступлений в области информационной безопасности, многие из которых не связаны непосредственно с компьютерной техникой.

В Оксфордском словаре, например, приставка «cyber» определяется как составная часть слов, «связанных с электронными коммуникационными сетями, особенно с интернетом» [4].

Первый международный договор, касающийся преступлений, «совершаемых через Интернет и другие компьютерные сети», – Конвенция Совета Европы 2001 года (Budapest, 23/11/2001, ETS No.185), именуется «Convention on Cybercrime» [5]. Интересно при этом, что в русском неофициальном переводе на том же сайте Совета Европы этот документ именуется Конвенцией «О компьютерных преступлениях» [6], что очевидно неточно.

Конвенция 2001 года (с дополнительным протоколом) подразделяет все киберпреступления на 5 групп:

– преступления против конфиденциальности, целостности и доступности компьютерных данных и систем («компьютерные преступления»);

– преступления, связанные с использованием компьютерных средств (подлог, мошенничество);

– преступления, связанные с контентом (содержанием данных) – детская порнография и т.п.);

– преступления, связанные с нарушением авторского права и смежных прав;

– преступления, посягающие на общественную безопасность (кибертерроризм, акты расизма и ксенофобии) [5].

В некоторых международных актах применяется метод установления обязанности государств – участников устанавливать в национальном законодательстве в качестве уголовно-наказуемых совокупность деяний, без определения содержания объединяющей их общей дефиниции. Так, например, в Конвенции ООН против коррупции 2003 года не дается определения коррупции, а перечисляется открытый перечень деяний, подлежащих уголовному наказанию [7].

Заключение. В силу неоднозначности трактовки понятия «киберпреступность» как правового и криминологического термина, можно предложить подход, аналогичный примененному в Конвенции против коррупции, рассматривая термин киберпреступность в качестве обобщающей дефиниции, означающей совокупность деяний, направленных против информационной безопасности, определенных, в частности, в вышеназванной Конвенции Совета Европы.

Существует, также, очевидная необходимость в разработке в рамках ООН современной Конвенции по противодействию киберпреступности, с закреплением в ней необходимых правовых понятий, связанных с киберпреступностью.

1. Салвадорская декларация о комплексных стратегиях для ответа на глобальные вызовы: системы предупреждения преступности и уголовного правосудия и их развитие в изменяющемся мире [Электронный ресурс].- Режим доступа: https:// www.un.org / ru / documents / decl_conv / declarations / salvador_declaration.shtml– Дата доступа: 22.02.2020.
2. Потери организаций от киберпреступности [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/.- Дата доступа: 22.02.2020.
3. Уголовный кодекс Республики Беларусь 9 июля 1999 г. № 275-З: принят Палатой представителей 2 июня 1999 года: одобрен. Советом Республики 24 июня 1999 года // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Республики Беларусь. – Минск, 2020.
4. Definition of cyber [Электронный ресурс].- Режим доступа // https:// www.oxfordlearnersdictionaries.com / definition / english /cyber.- Дата доступа: 22.02.2020.
5. Convention on Cybercrime [Электронный ресурс].- Режим доступа // https: // www.coe.int / en/web /conventions/full-list/-/conventions/treaty/185. – Дата доступа: 22.02.2020.
6. Конвенция о компьютерных преступлениях [Электронный ресурс]. – Режим доступа: https://rm.coe.int/1680081580. – Дата доступа: 22.02.2020.
7. Конвенция Организации Объединенных наций «Против коррупции» 31.10.2003 №58/4 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Республики Беларусь. – Минск, 2020.

РОЛЬ И ЮРИДИЧЕСКИЕ ВОЗМОЖНОСТИ МЕДИАЦИИ В УРЕГУЛИРОВАНИИ СПОРОВ

Тишурова А.В.,
магистрант ВФ ФПБ «МИТСО», г. Витебск, Республика Беларусь
Научный руководитель – Бочков А.А., канд. филос. наук, доцент

В настоящее время медиация является альтернативой не только государственному, но и арбитражному (третейскому) судопроизводству и представляет собой совершенно новый способ посредничества, специально разработанный для урегулирования конфликтов.