Вестник Сибирского юридического института МВД России

УДК 343.9

Елена Викторовна ХРИСТИНИНА,
доцент кафедры государственного и муниципального управления и таможенного дела Омского государственного технического университета, кандидат юридических наук
elena.nikitina83@mail.ru

К ВОПРОСУ ОБ УГОЛОВНО-ПРАВОВОМ ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

ON THE ISSUE OF CRIMINAL JUSTICE RESPONSE TO CYBERCRIME

В статье обосновывается существование в уголовном праве понятия «киберпреступность», проводится соотношение понятий «киберпреступление» и «компьютерное преступление», сформулировано авторское понятие данных явлений, на основе анализа специальной юридической литературы приводится авторская классификация киберпреступлений.

The article considers the existence in Criminal law the concept of «cyber-crime", the correlation of the concepts of «cybercrime» and «computer crime» is carried out, the author's concept of these phenomena is formu-lated, based on the analysis of special legal literature the author's classifi-cation of cybercrimes is given.

Ключевые слова: киберпреступление, информационное преступление, кибертехнологии, киберпространство, сеть «Интернет», компьютерная информация, информационно-телекоммуникационные технологии, уголовная ответственность.

Keywords: *cybercrime, information crime, cybertechnology, cyberspace, Internet, computer information, information and telecommunications technologies, criminal liability.*

Сегодня с учетом развития кибернетики, представляющей составную часть научно-технического прогресса, в любой области деятельности человека используются современные кибертехнологии. Значимость информационных технологий подтверждается принятием на государственном уровне Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы[1].

Появился особый вид преступлений – киберпреступления, которые имеют транснациональный характер. В настоящий период констатируется рост компьютерных преступлений. Так, в 2020 г. зарегистрированы 510,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 73,4% больше показателя 2019 г. За 9 месяцев 2021 г. зарегистрированы почти 403 тысячи указанных деяний, рост к аналогичному показателю 2019 г. составляет 11% В общем числе зарегистрированных преступлений их удельный вес составил 25% в 2020 г., 26,5% за 9 месяцев 2021 г.[2]

1 О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы : Указ Президента РФ от 09.05.2017 N 203 // Российская газета. 2017. 10 мая.

2 Официальный сайт МВД: состояние преступности. URL: ttps://мвд.рф/reports (дата обращения: 17.11.2021).

Используя возможности кибертехнологий, особенно в сети Интернет, доступность, небольшую стоимость информационных технологий, преступники получили разнообразные способы извлечения незаконной прибыли.

Однако в статьях Уголовного кодекса РФ нет понятия «киберпреступление», так как статьи уголовного закона содержат составы информационных преступлений, где отражаются вопросы преступного использования информационных технологий или средств компьютерной техники. Поэтому сфера киберпреступности остается нерегулируемой российским законодательством, хотя она имеет важное значение в осуществлении уголовной политики государства. Следовательно, в уголовном законе киберпреступления отождествляются с компьютерными преступлениями, где используются информационные технологии или средства компьютерной техники, что является сомнительным, так как правовая природа киберпреступности тесно взаимосвязана с наукой кибернетикой.

Различие понятий «киберпреступление» и «информационное преступление» можно провести по объекту и предмету преступного посягательства. Объектом компьютерных преступлений выступают общественные отношения, возникающие по обеспечению целостности и доступности электронной информации, а также сохранности компьютерных средств, необходимых для ее обработки. Предмет компьютерных преступлений представлен средствами хранения, обработки или передачи компьютерной информации. Объект и предмет киберпреступлений значительно шире, так как преступления могут совершаться с применением не только компьютерных средств, но и других технических устройств, причем предметом преступного посягательства может выступать виртуальная информация, находящиеся в сети Интернет.

Понятие «компьютерное преступление», используемое законодателем, обусловлено целесообразностью его употребления в криминалистических целях, например при организации расследования преступления, когда изучается личность преступника и способ совершения преступления.

В УК РФ закреплена глава 28, содержащая составы преступлений, устанавливающие уголовную ответственность за совершение противоправных деяний в отношении компьютерной информации. Таким образом, сфера уголовно-правового регулирования главы 28 состоит в обеспечении безопасности компьютерной информации и компьютерных систем.

Но в УК РФ есть составы преступлений, где компьютерная информация может быть средством совершения преступления, они расположены в других главах УК РФ. Такими преступлениями, совершаемыми в сети Интернет, могут быть мошенничество в сфере компьютерной информации, незаконные организация и проведение азартных игр, совершение незаконных финансовых операций, незаконный сбыт наркотиков с использованием средств Интернета, распространение порнографических материалов и ряд других составов. Поэтому назрела необходимость видоизменить главу 28 УК РФ, включив понятие «киберпреступление» и добавив дополнительные составы.

Российская уголовная доктрина в категорию информационной преступности включает разнообразные преступные деяния, посягающие на информацию и информационную среду. Е.В. Пискунова относит к компьютерным преступлениям такие общественно опасные и противоправные деяния, как преступления с применением информации, информационных технологий в качестве средств совершения; неправомерный доступ и распространение охраняемых законом информационных сведений, неправомерное сокрытие информации, неправомерное использование информации [1, с. 249]. Вышеуказанная классификация преступлений лишь частично определяет разновидности киберпреступности, которая возникает в киберпространстве с применением кибернетических технологий.

Важно указать, что в ходе применения термина «киберпреступность» с точки зрения рассмотрения лишь компьютерных преступлений возникает искажение этого понятия, так как оно не охватывает ряд важнейших

составов преступления. К примеру, в число киберпреступлений надлежит включить противоправные деяния, совершаемые с использованием мобильных устройств, в виде распространения детской порнографии или совершения мошеннических действий, связанных с оплатой услуг сотовой связи и прочие деяния. Следовательно, термин «киберпреступность» может быть рассмотрен с широкой точки зрения и охватывать различные преступные деяния, совершенные не только в информационно-телекоммуникационной сфере, где информация, информационные ресурсы, компьютерная техника могут являться предметом преступления, но и преступления, совершаемые в глобальной системе Интернет, где информация становится средством или орудием совершения преступного деяния.

В целом киберпреступления – это умышленные преступления, выражающиеся в виде незаконных действий (бездействий), совершенные с использованием кибертехнологий в виртуальной среде (киберпростанство) с применением телекоммуникационных способов и средств, в том числе сети Интернет, которые выступают преступными орудиями или предметами противоправных посягательств.

Под киберпространством понимаются информационно-телекоммуникационные сети, компьютерные локальные сети, глобальная сеть Интернет. Киберпространство является доступным для каждого информационного пользователя, что позволяет преступнику, находясь на территории одного государства, совершить преступление в отношении иностранных граждан, тем самым преступление имеет транснациональный характер.

Кибертехнологии – технические средства (персональные компьютеры, ноутбуки, смартфоны) и сама информация и ее носители.

Следует обратиться к международному опыту применения термина «киберпреступность», который был впервые представлен еще в 1986 г. в Париже группой экспертов Организации экономического сотрудничества и развития, где киберпреступление определялось как любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных[3].

Уже позже, на X Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями, состоявшемся в Вене 10-17 апреля 2000 г., было четко сформулировано понятие киберпреступности, которое означало «любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети»[4].

Таким образом, киберпреступления на основании представленного понятия можно рассмотреть в узком и широком смысле.

Киберпреступление в узком понимании – это любое противоправное деяние, которое совершается путем проведения электронных операций, целью которого выступает получение доступа к компьютерным системам и информационным данным.

Киберпреступление в широком понимании – это любое преступление, совершаемое в компьютерной системе или глобальной сети, состоящее из незаконного хранения, распространения электронной информации.

Следует отметить, что в определение киберпреступности включается также противоправное вмешательство в компьютерные средства, программы и сети, несанкционированная модификация компьютерных сведений, другие противоправные действия, совершенные с использованием компьютеров, компьютерных сетей и программ.

Важным международным документом по борьбе с киберпреступностью выступает Конвенция о преступности в сфере компьютерной информации ETS N 1857

3 OECD, Computer – Relates Crime: Analysis of Legal Policy. Paris, 1986.

4 Справочный документ для семинара-практикума по использованию компьютерной сети «Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями» // Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями : сборник документов. М., 2002.

(далее – Будапештская конвенция)[5], где применяется термин cybercrime (киберпреступление) и cyberspace (киберпространство).

На основании Европейской конвенции киберпреступления – это правонарушения, которые направлены против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также неправомерное их применение.

Кроме представленных определений Советом Европы был выделен перечень киберпреступлений против конфиденциальности, целостности и допустимости компьютерных данных и систем: незаконный доступ (ст. 2), незаконный перехват (ст. 3), вмешательство в данные (ст. 4), вмешательство в систему (ст. 5)[6].

Разделение киберпреступлений на виды возможно проводить по предмету, цели и способу совершения преступления:

1) преступления, совершенные в информационно-телекоммуникационной сфере. Предметом преступления является информация, информационные ресурсы, компьютеры. Цель совершения преступления – завладение, изменение или уничтожение информации, находящейся в компьютере, или неправомерное подключение к сети. Способ совершения преступления: незаконное изъятие информации или ее копирование;

2) киберпреступления, совершаемые в киберпространстве с использованием кибертехнологий. Предметом преступления являются денежные средства, информация, оружие, наркотики и прочее. Цель совершения преступления может быть разнообразной в зависимости от совершаемого деяния (например, мошеннические действия, совершаемые с использованием мобильных устройств, имеют целью хищение денежных средств путем обмана или злоупотребления доверием). Способ совершения преступления: использование определенных средств или орудий (допустим, мошенничество в области интернет-продаж и покупок).

Отличительным признаком киберпреступлений является высокотехнологичный характер, состоящий в применении современных кибертехнологий, информационно-коммуникационных сетей, компьютерной техники, которые выступают в качестве средств и орудий совершения данных преступных деяний.

В настоящее время отмечается сложность в расследовании киберпреступлений, так как большая часть из них имеет латентный характер, что объясняется разными причинами: нежелание потерпевшего обращаться с заявлением в правоохранительные органы, сложность выявления и доказывания вины киберпреступников, тесная связь преступника с организованными преступными группами. Это объясняется и сложностью установления личности преступника, обладающего необходимыми знаниями, навыками в сфере компьютерных технологий и тщательно маскирующего электронные следы преступления.

Кроме того, с развитием различных кибертехнологий, увеличением пользователей в системе Интернет, развитием средств мобильной связи, систем электронного документооборота появляются новейшие способы совершения киберпреступлений. Следовательно, киберпреступления могут происходит в различных сферах: экономической, политической и социальной. Большая часть киберпреступлений совершаются в экономической сфере, например мошенничество с использованием интернет-банкинга (технология банковского обслуживания, при которой предоставляется доступ к счетам и банковским операциям («сбербанк-онлайн»)) или банковский фишинг (разновидность интернет-мошенничества с целью завладения доступа к конфиденциальным информацией пользователя: логинам и паролям, осуществляется посредством массовых рассылок электронных писем от имени различных популярных организаций).

Большую общественную опасность представляет киберпреступность в политической

5 Convention on Cybercrime. URL: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (дата обращения: 23.06.2021).

6 Преступления, связанные с использованием компьютерной сети / X конгресс ООН по предупреждению преступности и обращению с правонарушителями // A/CONF. 187/10.

сфере, когда хакеры, спецслужбы иностранных государств, экстремистские и террористические организации осуществляют кибератаки на сайты органов государственной власти, кибершпионаж в отношении сведений, составляющих государственную тайну, распространение информации экстремистского содержания, вербовку граждан в террористические организации.

Эксперты международной компании Group-IB, специализирующейся на предотвращении кибератак, создали новую парадигму информационной безопасности, куда включили самые распространение киберпреступления:

– хакерские действия, нацеленные на обеспечение долгого присутствия в сетях объектов критической инфраструктуры с целью саботажа и шпионажа за организациями из различных секторов;

– хакерские действия, нацеленные на хищение денежных средств со счетов финансовых организаций;

– мошенничество с банковскими картами физических лиц;

– хакерские действия, нацеленные на хищение криптовалюты с криптобирж;

– хакерские атаки, нацеленные на поиск уязвимости в практической реализации криптосистемы и уязвимости микропроцессоров разных вендоров (side-channel атаки)[7].

Ряд перечисленных деяний не нашли отражения в УК РФ. Таким образом, существует необходимость совершенствования уголовно-правового регулирования в части включения в УК РФ понятия киберпреступления, а также введения новых составов киберпреступлений, возникающих при использовании преступниками новых кибертехнологий (компьютерный подлог, компьютерный саботаж, несанкционированный перехват данных, хищение криптовалюты).

7 Официальный сайт международной компании Group-IB. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/ (дата обращения: 23.06.2021).

Библиографический список

1. Пискунова, Е.В. Информационная преступность: уголовно-правовые и криминологические аспекты / Е.В. Пискунова // Государство и право в новой информационной реальности : сборник научных трудов / РАН. ИНИОН. Центр социал. науч.-информ. исслед. Отд. правоведения; Рос. гос. ун-т правосудия. – М., 2018. – С. 249-250.