опасность. Большинство правонарушений и мелких проступков перестали считаться преступлениями, что свидетельствовало о широком распространении декриминализации деяний. С этого момента перестало допускаться распространение закона на случаи, непосредственно им не регулируемые. Важнейшее словосочетание «предусмотренное уголовным законом» подчеркивало недопустимость аналогии в уголовном праве.

Безусловно, наука уголовного права современной России негативно относится к применению аналогии в уголовном праве. Запрет такого применения является прямым следствием положений, закрепленных в ч. 1 ст. 3 УК РФ, но законодатель посчитал целесообразным сделать акцент на этой проблеме, долгие годы существовавшей в уголовном праве СССР, и напрямую закрепил этот запрет в ч. 2 ст. 3 УК РФ.

Таким образом, как показывает опыт СССР, применение уголовного закона по аналогии долгое время было разрешено на законодательном уровне. Но все случаи подобного применения приводили только к печальным последствиям, когда искажался дух закона, оставалась лишь его буква. Неблагоприятные последствия применения аналогии в уголовном праве как в публично-правовой отрасли проявляются до сих пор. Аналогия уголовного права в советские годы нарушала принцип законности, а не восполняла пробелы в законодательстве. В современном российском уголовном законодательстве аналогия закона является запрещенной и недопустимой потому, что ее применение нарушило бы каждый из принципов, законодательно закрепленных в ст. 3-7 УК РФ. Дозволение применять уголовную норму по аналогии означает нарушение закона.

Чавлытко А.А.

Калининградский филиал Санкт-Петербургского университета МВД России
Научный руководитель А.О. Астахова, кандидат юридических наук

К вопросу понятия киберпреступности

В настоящее время достаточно сложно представить нашу жизнь без компьютеров, телефонов и других электронных устройств, которые в связи с модернизацией и развитием все больше заполняют собой повседневную жизнь. По состоянию на 2021 г. мобильными устройствами пользуется 66,7% пользователей со всего мира, что составляет 5,22 миллиарда человек. С учетом стремительного роста количества пользователей прямо пропорционально развивается и увеличивается количество преступлений, расширяются методы совершения преступлений с использованием информационных технологий.

В результате неправомерных деяний, совершаемых при помощи различных устройств электронных устройств, нарушаются или ограничиваются имущественные права граждан, что образует состав рассматриваемого явления – киберпреступления.

Киберпреступность (киберпреступления) не имеет единой законодательно закрепленной дефиниции. По нашему мнению, киберпреступление (от англ. cybercrime) – это виновно совершенное и уголовно наказуемое общественно-опасное деяние, происходящее в виртуальном пространстве с использованием информационных технологий и глобальных сетей.

Следует еще различать термин «компьютерное преступление», которое имеет более узкую направленность, в связи с тем, что для совершения такого рода преступления необходим компьютер, а для совершения «киберпреступления» – любое иное телекоммуникационное устройство, компьютеры, сотовая связь и прочее, именно поэтому к феномену киберпреступности относится и мошенничество, совершаемое по телефону.

Исходя из этого, следует, что компьютерное преступление является составляющей явления киберпреступности, это более узкое понятие, к которому относится ряд составов, например ст. 272 УК РФ.

Учитывая отсутствие в законодательстве четкого определения понятия «киберпреступление», УК РФ предусматривает уголовную ответственность за связанные с данным явлением виновно совершенные опасные деяния. Анализируя главу 28 УК РФ, посвященную преступлениям в сфере компьютерной информации, можно заметить тот факт, что в ссылках на постановления Пленума Верховного Суда нет ни одной из тех, которая была бы посвящена конкретно преступлениям, связанным с информационными технологиями.

Отсутствие единой терминологии не влияет на наличие составов преступлений, описывающих преступные деяния, непосредственно осуществляемые при помощи различных девайсов. Например, ст. 159.6 УК РФ предусматривает ответственность за мошенничество в сфере компьютерной информации, при этом не содержит толкования термина «компьютерная информация», лишь примечание к ст. 272УК РФ дает нам определение.

Киберпреступность напрямую связана с сетью Интернет и в связи с рядом свойств имеет достаточно широкое распространение.

Учитывая то, что Интернет – это система связанных между собой устройств, следует принять во внимание тот факт, что его наличие позволяет человеку из любой точки мира анонимно (тайно) совершать какие-либо преступные действия. Помимо этого, лицо может совершать неограниченное количество преступлений, находясь удаленно от субъекта посягательства. Также в настоящее время существует ряд способов, позволяющих скрыть свое местоположение, что усложняет процесс расследования такого рода преступлений. Сделать это возможно при помощи VPN – программного обеспечения, которое

позволяет сохранять конфиденциальность и скрывает реальное местоположение пользователя, оно шифрует подключение пользователя к сети, что не позволяет определить место его подключения[1].

Также характеризуя преступления, совершаемые в информационной сфере, стоит отметить отсутствие необходимости оказывать какое-то физическое воздействие и применять физическую силу, что, вероятно, привлекает лиц к данному виду преступлений. Еще одним мотивирующим фактом на совершение данного рода преступлений является недостаточная изученность всех способов совершения преступлений, неполная правовая регламентация в виде отсутствия единой терминологии и полного, ясного разграничения составов преступления, а также низкий уровень материально-технического обеспечения подразделений, осуществляющих расследование преступлений.

Чаще всего киберпреступность связана с тем, что из-за низкого уровня правовой грамотности и в целом осведомленности в сфере информационных технологий пострадавшие даже не знают о том, что стали жертвой преступления. Также причиной распространенности данного вида преступлений является частичное отсутствие реальной возможности осуществлять профилактику и предупреждение роста преступности привычными методами.

Исследователи[2] выделяют ряд факторов, способствующих совершению киберпреступлений.

1. Объективные факторы – информационная среда и ее инфраструктура (повсеместность использования соответствующей инфраструктуры, сетей, программ, оборудования, а также растущее во всем мире и в России количество пользователей программно-технических средств; доступность компьютерных технологий; возрастающая зависимость современных технологий от компьютерных систем и средств телесвязи; широкое использование зарубежного программно-технического обеспечения, операционных систем, а также технических компонентов).

2. Факторы, относящиеся к особенностям преступности в сфере компьютерных технологий (преступник может находиться в одной стране, преступление совершать в другой, а последствия преступления могут наступать в третьей, что затрудняет противодействие преступности в рамках одного государства и даже совокупности государств; возможность при совершении преступлений в сфере компьютерных технологий одновременно атаковать сотни и тысячи компьютеров, находящихся как в одной, так и в разных странах;

---

[1] Что такое VPN и для чего он нужен. URL: https://trends.rbc.ru/trends/industry/604f0a309a79477d332569e3.

[2] См., напр.: Бугаев В.А., Чайка А.В. Факторы преступности в сфере компьютерных технологий // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2019. № 4. С. 139-145. URL: https://cyberleninka.ru/article/n/faktory-prestupnosti-v-sfere-kompyuternyh-tehnologiy (дата обращения: 15.11.2021).

многообразие способов совершения преступлений в сфере компьютерных технологий, возможность совершения преступлений в автоматических режимах и объединения ресурсов пользователей помимо их желания и воли; невозможность предотвращения и пресечения преступлений в сфере компьютерных технологий традиционными способами; отсутствие какой-либо достоверной статистики преступности в сфере компьютерных технологий, ее состояния, структуры и динамики; чрезвычайно широкая распространенность преступлений в сфере компьютерных технологий и высоколатентный характер данных преступлений, обусловленный самыми разными причинами; неустоявшаяся судебно-следственная и прокурорская практика).

3. Субъективные факторы преступности в сфере компьютерных технологий, относящиеся к субъектам общественных отношений, возникающих по поводу обеспечения информационной безопасности (несоответствие системы международных стандартов в области компьютерной техники, связи и информационной безопасности требованиям времени; отсутствие должного международно-правового сотрудничества в сфере противодействия преступности в сфере компьютерных технологий; отсутствие комплексных государственных мер, направленных на противодействие преступлениям в указанной сфере; недостатки действующего информационного законодательства, страдающего отсутствием системности и планомерности развития и законодательного регулирования; несоответствие уголовного законодательства существующим общественно опасным явлениям в информационной сфере; несовершенство действующего уголовного законодательства; несовершенство социальных, юридических и политических структур, уровень развития которых значительно отстает от уровня развития компьютерных и телекоммуникационных технологий; недостаточное правовое, научное, организационно-техническое и правоприменительное противодействие преступности в сфере компьютерных технологий; недостаточная осведомленность общества об уязвимости компьютерных систем и необходимость осуществления действенных мер безопасности; неадекватное отношение общества к преступности в сфере компьютерных технологий в целом и компьютерным преступникам в частности; недостаточное правовое воспитание населения, особенно подрастающего поколения).

Подводя итог, отметим, что киберпреступность – это негативное правовое явление, включающее в себя совокупность преступлений, совершаемых при помощи различных устройств, чаще всего со злоупотреблением доверием, имеющее широкое распространение в связи с анонимностью и удаленностью преступника, малой осведомленностью граждан и отсутствия определенных методов борьбы с преступлениями и мер профилактики.