КИБЕРПРЕСТУПНОСТЬ КАК ГЛОБАЛЬНАЯ УГРОЗА СОВРЕМЕННОСТИ

М.Г. Головенчик
преподаватель УО «Юридический колледж Белорусского государственного университета»

Последние несколько десятилетий отмечаются глобальным прорывом в области развития информационных и телекоммуникационных технологий. Весь этот процесс, получивший в литературе ёмкое понятие «цифровизация» [1], направлен на упорядочение производственных операций, облегчение взаимодействия между участниками социальных и правовых отношений, а в целом – на разработку и унификацию единых алгоритмов, посредством которых вся окружающая нас информация подлежит переводу в бинарный код, который впоследствии становится легко читаемым современными техническими устройствами.

Вместе с тем, вся история развития человеческой цивилизации показывает, что любое научно-техническое достижение, решение, изобретение и проч. могут использоваться не только на пользу обществу, но и во вред ему. Не являются исключением и разработки в области информационных технологий. В то время как одни члены общества получают удовлетворение от использования всех благ современного технического прогресса, другие используют эти же блага для достижения совсем иных – преступных целей. Примеров совершения противоправных деяний, сопряженных с использованием современных средств коммуникации и связи, более чем достаточно: мошенническое завладение денежными средствами путем неправомерного получения удаленного доступа к ним, противоправное использование сведений составляющих личную тайну граждан, саботаж нормальной работы государственных органов, предприятий, учреждений, организаций и проч. На одном из последних заседаний коллегии Следственного комитета Республики Беларусь было отмечено, что только за последний отчетный год относительный показатель преступлений, совершенных с использованием компьютерной техники и направленных против информационной безопасности, увеличился в два раза и превысил 12%. В этой связи совершенствование работы по противодействию преступлениям в сфере высоких технологий было определено главой Следственного комитета Республики Беларусь в качестве приоритетного направления в деятельности данного органа на 2020 год [2].

Несмотря на значительность угрозы киберпреступности и ее распространенность по всему миру, вплоть до настоящего времени ученым не удалось выработать четкого представления о том, что необходимо считать киберпреступлением. На сегодняшний день на страницах специальной литературы можно обнаружить лишь попытки выявить и обосновать те или иные признаки такого преступного деяния, а существующие нормативные документы чаще всего идут по пути формирования некоторого списка

противоправных деяний, которые надлежит квалифицировать таким образом. Так, по мнению белорусских ученых В.В. Белокопытова и В.М. Филиппенкова киберпреступлением следует считать «вид правонарушения, непосредственно связанного с использованием компьютерных технологий и сети Интернет, включающий в себя распространение вирусов, нелегальную загрузку файлов, кражу персональной информации, например, информации по банковским счетам». К киберпреступлениям, с точки зрения указанных авторов необходимо относить только такие противоправные деяния, «в которых ведущую роль играют компьютер или компьютерная сеть» [3].

Несмотря на, в целом, верную попытку обозначить круг деяний, характеризуемых как киберпреступность, подобное определение не содержит всех необходимых признаков, по которым то или иное преступление следует относить к разряду киберпреступлений. Это прослеживается уже в том, что понятия «использование компьютера» и «использование компьютерных технологий» на сегодняшний день уже нельзя рассматривать как тождественные. Так, И.Г. Чекунов справедливо обращает внимание на то, что современные гаджеты являются достаточным средством для того, чтобы совершить киберпреступление через телекоммуникационные системы и сети [4, с. 54]. Понятие «компьютер» сегодня не должно ограничиваться привычным пониманием его как набора взаимосвязанных элементов (системный блок, клавиатура, монитор и т.д.), а вывод о признании того или иного устройства компьютером должен делаться исходя из тех функциональных возможностей, которые данное устройство предоставляет его обладателю. В частности, к такому функционалу следует отнести возможность подключения к телекоммуникационным сетям и осуществление там действий, связанных с размещением, получением или модификацией информации.

Кроме того, принципиально значимым является вопрос о режиме совершения противоправного деяния – «online» или «offline». В зависимости от ответа на данный вопрос необходимо осуществлять следующую градацию преступлений рассматриваемой группы – противоправные деяния, совершенные «offline» следует квалифицировать как компьютерные преступления, но в то же время к числу киберпреступлений их относить нельзя. На этом основании нужно сделать вывод о том, что компьютерные преступления и киберпреступления следует соотносить как целое и часть – киберпреступления являются составной частью компьютерных преступлений, но не ограничивают последние [5, с. 43].

Также в число признаков киберпреступления следует включить характеристику элементов субъективной стороны, поскольку такие преступления могут быть совершены только умышленно. При этом представляется, что умысел лица может быть как прямым, так и косвенным. Так, преследуя цель завладения чужим имуществом, виновное лицо через глобальную сеть Интернет проникает в базу данных коммерческого банка, где, посредством видоизменения хранящейся там информации, «перечисляет» на

интересующий его счет денежную сумму. Виновный действует с прямым умыслом, осознавая общественно опасный характер своего деяния, предвидя неизбежность наступления общественно опасных последствий и желая наступления таких последствий. В ином случае виновный модифицирует компьютерную информацию о движении поездов, что приводит к коллапсу на определенном транспортном узле. В подобной ситуации виновный осознает общественную опасность своего деяния, выразившегося в неправомерном доступе к компьютерной информации и ее модификации, предвидит возможные последствия и безразлично относится к наступлению любого их вида.

Таким образом, к числу признаков киберпреступления следует отнести: 1) использование информационно-коммуникационных технологий как средства совершения преступления; 2) модификация цифровой информации в режиме «online»; 3) наличие умысла на совершение противоправного деяния. Исходя из этих признаков, представляется возможным сформулировать следующее определение киберпреступления – это умышленное дистанционное посягательство на охраняемые уголовным законом общественные отношения, совершенное посредством использования информационно-телекоммуникационных технологий. Также следует отметить, что одним из важных криминолого-криминалистических признаков киберпреступления является его трансграничный характер. Изменяя цифровую информацию, лицо, находясь в одной точке земного шара, может причинить вред охраняемому объекту, находящемуся под защитой внутреннего законодательства иного государства. В этой связи для должного противодействия распространению киберпреступности требуются совместные усилия государств.

Характеризуя межгосударственные усилия, направленные на борьбу с проявлениями трансграничной киберпреступности, следует отметить, что на сегодняшний день большинство мировых держав понимают опасность этого явления и предпринимают определенные шаги к тому, чтобы противостоять ей. Вместе с тем, нельзя не отметить, что, во-первых, вплоть до настоящего времени не было разработано единого международного документа, посвященного данной проблеме – все существующие международные соглашения в этой области носят лишь региональный характер. Во-вторых, даже имеющиеся дву- и многосторонние соглашения, распространяющие свое действие на определенный регион, как правило, существенно отстают в своем правовом регулировании от стремительно развивающегося технического прогресса. Внесение же соответствующих изменений и дополнений требует прохождения значительных бюрократических процедур, что подчас нивелирует актуальность правовых документов. Достаточно отметить, что в сентябре 2018 года было подписано Соглашение государств-участников СНГ о сотрудничестве в борьбе с преступлениями в сфере информационных технологий [6]. Вместе с тем, потребовалось около полутора лет для того, чтобы Соглашение вступило в законную силу. В соответствии с нормами

Соглашения государства-участники должны были провести внутренние процедуры, предусмотренные их национальным законодательством, направленные на имплементацию норм Соглашения во внутригосударственное законодательство. Однако третий необходимый участник Соглашения, выполнивший условие по извещению депозитария о прохождении имплементационной процедуры, сделал это только в феврале 2020 года, после чего потребовался еще месяц для того, чтобы Соглашение обрело свой надлежащий юридический статус.

Таким образом, для успешной борьбы с международной киберпреступностью, которую, без сомнения, можно отнести к числу глобальных проблем современности, требуется, во-первых, унификация подходов к пониманию самой сущности этого явления, во-вторых, активизация усилий всех, без исключения государств, направленных на оперативную модернизацию внутреннего законодательства и разработку глобального международного соглашения, нормы которого регулировали бы складывающиеся отношения в рассматриваемой сфере.

Библиографический список

1. Цифровизация, промышленный интернет вещей и Индустрия 4.0. Кратко // Газпром [Электронный ресурс]. – Режим доступа: https://neftegaz.ru/tech-library/menedzhment/142438-tsifrovizatsiya-promyshlennyy-internet-veshchey-i-industriya-4-0-kratko/. – Дата доступа: 08.11.2020.

2. Год борьбы с киберпреступлениями. На заседании коллегии Следственного комитета поставлены задачи на 2020 год // Следственный комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: https://sk.gov.by/ru/news-ru/view/god-borby-s-kiberprestuplenijami-na-zasedanii-kollegii-sledstvennogo-komiteta-postavleny-zadachi-na-2020-god-8809/. – Дата доступа: 08.11.2020.

3. Белокопытов, В.В. Особенности совершения и предупреждения киберпреступлений / В.В. Белокопытов, В.М. Филиппенков // Консультант Плюс: Беларусь [Электронный ресурс]. – Минск: ЮрСпектр, 2020.

4. Чекунов, И.Г. Понятие и отличительные особенности киберпреступности / И.Г. Чекунов // Российский следователь. – 2014. – № 18. – С. 53-56.

5. Бытко, С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершаемые с использованием компьютерных технологий: Дис. … канд. юрид. наук / С.Ю. Бытко. – Саратов, 2002. – 204 с.

6. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Заключено в г. Душанбе 28.09.2018) // Национальный правовой Интернет-портал Республики Беларусь. – 01.08.2019. – 3/3682.