Арестов Александр Вячеславович
студент
Научный руководитель
Куликов Александр Викторович
заслуженный юрист РФ, д-р юрид. наук,
профессор, заведующий кафедрой
ФГАОУ ВО «Балтийский федеральный
университет им. И. Канта»
г. Калининград, Калининградская область

DOI 10.31483/r-106755

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПНЫХ ДЕЯНИЙ ПО СТАТЬЯМ 272 И 273 УК РФ

Аннотация*: в статье приводится общая характеристика и анализ уголовного законодательства в отношении ст. 272 и 273 УК РФ. Рассмотрен ряд проблем квалификации преступных деяний по названным статьям. Сделан обоснованный вывод о необходимости модернизации законодательства по данному вопросу и предложены возможные пути её проведения.*

Ключевые слова*: компьютерная информация, вирусная программа, ответственность лиц, программное обеспечение, неправомерный доступ, интернет-ресурсы.*

Жизнь современного человека неразрывно связана с компьютерными и информационными технологиями. Их применение позволяет существенно ускорить процесс обмена данными, а значит, сделать нашу бытность в разы эффективнее в самых различных сферах – медицине, науке, искусстве, и конечно, в сфере государственного регулирования. Для правоприменителя возможность быстро получать и отправлять информацию имеет огромное значение – ведь это позволяет в кротчайшие сроки реализовывать гражданские права, поименованные в Конституции Российской Федерации. Невозможно не согласиться с тем,

что удобство работы с информацией вышло на качественно новый для пользователя уровень, это касается как создания, так и последующего доступа к информации. Однако нельзя упускать из внимания тот факт, что это явление также стало причиной появления новых рисков и угроз, которые ранее не были известны как обществу, так и законодателю.

Преступления в сфере компьютерной информации по сути своей представляют общественно опасные деяния, которые причиняют вред (или создают угрозу его причинения) безопасности хранения, использования или распространения информации, или ресурсов, непосредственно содержащих информацию [5]. Необходимо отметить, что борьба с преступностью для достижения эффективной её реализации должна иметь комплексный подход, в котором находят отражение организационные, общественные, тактические, политические, и конечно, идеологические методы. Однако без должной нормативно-правовой базы всё это не сможет должным образом функционировать и привносить в правоприменительную практику ожидаемых изменений. На основании этого считаем необходимым упомянуть о некоторых актуальных проблемах, существующих в статьях 272 и 273 УК РФ.

Анализ судебной практики, приведённый Гладких В.И., позволяет нам сделать вывод: зачастую действия в сфере компьютерной информации являлись именно способом совершения преступлений и за последние 9 лет вынесено большое количество приговоров по совокупности статей 272–274 УК РФ и других видов правонарушений [2]. Статистика показала, что из более 90 приговоров почти 30% из них это случаи, в которых преступление в сфере компьютерной информации было совершено с целью облегчить совершение другого преступления. Совершением преступных действий, предусмотренных статьями 272 или 273 УК РФ правонарушители получали возможность совершить такие правонарушения, как незаконное получение данных, составляющих коммерческую, налоговую или банковскую тайну (183 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), нарушение авторских и смежных прав

(ст. 146 УК РФ) и других правонарушений, представляющих собой доступ к защищённой законом информации.

Так, например, А., из корыстных побуждений разработал вредоносное (вирусное) программное обеспечение под видом сайта, фиктивно подражающего сайту одной из популярных платежных систем, а затем разместил его в сети Интернет. Далее, А. осуществлял незаконное копирование персональных данных пользователей, которые вводили свои данные на его сайте. Таким образом, им был получен доступ к паролям и логинам от счетов интернет-кошельков пользователей и возможность распоряжаться находящимися на них деньгами. Приговором от 9 ноября 2018 года А. был обвинён в совершении преступлений, предусмотренных пунктом «в» части 3 статьи 158 и, по совокупности, частью 2 статьи 273 УК РФ [3].

Считаю важным оставить ремарку о том, что на данный момент в Уголовном кодексе предусмотрены деяния, которые определённым образом, в частности, схожим объектом правонарушения и действиями злоумышленника, связаны с посягательством на компьютерную информацию. Примером могут послужить такие составы, как мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ). Однако такие преступления традиционно относят к киберпреступности, а потому предметом настоящего исследования не являются.

На практике возникают случаи, когда совершаемое преступное деяние в сфере компьютерной информации являлось «предтечей» для совершения целой серии преступлений. Особенно часто такие преступления совершаются лицами, имеющими доступ к защищенной информации (паспортным данным или данным от электронных платежных систем), что является деянием, предусмотренным ч. 3 ст. 272 УК РФ. Среди прочих можно выделить приговор от 13 декабря 2019 г. [4]. Согласно приговору, два лица были обвинены в совершении преступлений, предусмотренных ч. 2 ст. 272, ч. 3 ст. 183 УК РФ и п. «г» ч. 3 ст. 158 УК РФ. Мотивировочная часть приговора гласит, что суд признал обвиняемых ви-

новными в совершении по меньшей мере 20 краж в отношении электронных денежных средств, а также 7 эпизодов незаконного получения сведений, составляющих коммерческую, налоговую или банковскую тайну. Оба лица являлись сотрудниками банка, и открыли возможность совершения перечисленных правонарушений, неоднократно осуществив неправомерный доступ к компьютерной информации (ч.3 ст. 272 УК РФ), в виде конфиденциальных данных клиентов банка.

Считаем справедливым сделать вывод о том, что законодателю следует обратить внимание на роль серии преступлений в сфере компьютерной информации, как способа совершения иных преступлений, и отразить эту особенность в уголовном законе. Однако на сегодняшний день составы статей 272 – 274.2 УК РФ не включают в себя такой квалифицирующий признак, как намерение лица, совершившего деяние в данной сфере, совершить или скрыть другое преступление или получить доступ к его совершению. На наш взгляд – это принципиально важно, так как электронная среда, в которой и находится защищенная законом информация, в особенности Интернет-среда, отличается от той, в которой совершаются другие виды преступлений. Важно осознавать, что в ряде случаев лицо физически не может совершить определенное правонарушение без совершения уголовно-наказуемых действий, предусмотренных ст. 272 УК РФ. Вполне справедливо умозаключение о том, что законодателю необходимо учитывать мотив и цель злоумышленника при совершении преступления в сфере компьютерной информации. Так, на заре развития компьютерных технологий уничтожение или незаконное копирование данных, а также создание и распространение вирусного программного обеспечения, совершалось в основном из хулиганских побуждений, то на сегодняшний день такие деяния зачастую имеют ярко выраженный корыстный интерес, что необходимо учитывать при модернизации главы 28 Уголовного кодекса.

Кроме того, считаем важным обратиться к вопросу о введении в диспозицию статьи 272 УК РФ такой квалифицирующей новеллы, как совершение пре-

ступления с целью скрыть другое преступление или облегчить путь к его совершению. Такая правовая конструкция уже выражена законодателем как отягчающее обстоятельство в п. «е.1» ч. 1 ст. 63 УК РФ. Однако в ряде случаев законодатель вполне обоснованно посчитал, что такое обстоятельство должно быть выделено как квалифицирующий признак конкретного правонарушения. Примером может послужить убийство с целью скрыть другое преступление или облегчить его совершение, предусмотренное пунктом «к» ч. 2 ст. 105 УК РФ. На основании ранее изложенного, считаем необходимым данный квалифицирующий признак закрепить и в статье 272 УК РФ.

Проведенный нами анализ как актуального, так и уже утратившего силу уголовного законодательства и судебной практики позволил выделить также и ряд проблем, связанных конкретно со ст. 273 УК РФ: «Создание, использование и распространение вредоносных компьютерных программ». На сегодняшний день диспозиция данной статьи предусматривает такие виды активных действий как создание, распространение и использование вредоносного программного обеспечения. По данной статье преступление считается оконченным с момента совершения одного из указанных в диспозиции действий, наступление таких последствий как уничтожение, блокирование, модификация или копирование информации, или же причинение вреда средствам защиты информации не имеет значения для квалификации деяния. Однако на практике возникает следующая правовая неопределённость. Как было отмечено ранее, закон предусматривает ответственность за создание вирусной программы, но никак не предусматривает её за приобретение и получение / передачу в дар вирусной программы. Не вполне ясно, почему законодатель избрал именно такой подход, поскольку целью привлечения к ответственности лиц за создание вирусной программы явно свидетельствует о намерении криминализировать сам факт наличия вирусной программы в собственности у лица. В научной литературе встречается мнение, что привлечение к ответственности за создание вирусной программы и непривлечение за её приобретение обуславливается специальным субъектом преступления –

лицо, имеющее навыки в области программирования. Иной субъект попросту невозможен, так как нельзя разработать вредоносную компьютерную программу, не имея, собственно, навыков разработки вредоносной компьютерной программы. Однако «навыки в области программирования» – понятие довольно обширное и абстрактное, к ним относятся не только непосредственно навыки по написанию программного кода, но и навыки в сфере анализа данных, математики и маркетинга, которыми также может обладать лицо, приобретающее вирусную программу.

Исходя из вышеизложенного, считаем необходимым сделать вывод о том, что часть 1 ст. 273 УК РФ следует дополнить положением о криминализации не только создания, использования и распространения, но и приобретения вирусного программного обеспечения, ввиду не меньшей общественной опасности. В поддержку нашего мнения необходимо сказать, что такая позиция ранее высказывалась в научной среде [1].

Также нерешенным остаётся вопрос о том, необходимо ли наступление общественной опасности или её угроза для того, чтобы признать лицо виновным в создании вирусной программы. Так как состав преступления, согласно УК РФ – формальный, то ответственность по общему правилу должна наступать за сам факт создания вирусной программы. Однако помимо создания таких программ в преступных целях, лицо также может заниматься разработкой в научно-исследовательских или профилактических и превентивных целях. Положение ч. 2 ст. 14 УК РФ о малозначительности деяния, по нашему мнению, не применимо в рассматриваемом примере, в силу того, что данная дефиниция не имеет четко выраженных критериев допустимости и судебная практика по данной статье крайне мала. Следовательно, считаем важным также обозначить необходимость развития законодателем правового механизма, регламентирующего вопрос о том, является ли создание вирусной компьютерной программы преступным или нет в каждом конкретном случае.

Список литературы

1. Гребенкин Ф.Б. Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ / Ф.Б. Гребенкин, Л.А. Коврижных // Вестник гуманитарного образования. – 2017. – №2. – С. 71–77.

2. Гладких В.И. Проблемы совершенствования уголовно-правовых мер противодействия преступлениям в сфере компьютерной информации / В.И. Гладких, И.Н. Мосечкин // Всероссийский криминологический журнал. – 2021. – №2.

3. Приговор от 9 ноября 2018 г. по делу №1-588/2018 по обвинению Р. А. Г. в совершении преступлений, предусмотренных пунктом «в» части 3 статьи 158, частью 2 статьи 273 УК РФ // СПС «Консультант Плюс» (дата обращения 20.03.2023).

4. Приговор от 13 декабря 2019 г. по делу №1-268/2019 по обвинению М. Я. В и Г. В. Р. в совершении преступлений, предусмотренных частью 2 статьи 272, частью 3 статьи 183 УК РФ и пунктом «г» части 3 статьи 158 УК РФ // СПС «Консультант Плюс» (дата обращения 20.03.2023).

5. Чучаев А.И. Уголовное право. Особенная часть / А.И. Чучаев. – 2019. – Гл. 14, § 1.