УДК 343.1: 004.056 **Юридические науки**

Занкина Дарья Васильевна, *студентка юридического факультета,*
специальность «Правоохранительная деятельность»
МГУ им. Н.П. Огарева, Россия, г. Саранск

ПРОБЛЕМЫ КВАЛИФИКАЦИИ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: В статье рассматриваются вопросы квалификации преступлений, связанных с неправомерным доступом к компьютерной информации. Приводится статистика осужденных за последние годы. Раскрываются наиболее типичные проблемы квалификации данного вида преступлений, анализируются соответствующие примеры из судебной практики и предлагаются пути решения данных проблем.

Ключевые слова: компьютерная информация, неправомерный доступ, Интернет, уничтожение, модификация.

Annotation: The article deals with the issues of qualification of crimes related to illegal access to computer information. The statistics of convicts in recent years are given. The most typical problems of qualification of this type of crimes are revealed, relevant examples from judicial practice are analyzed and ways of solving these problems are proposed.

Keywords: computer information, unauthorized access, Internet, destruction, modification.

На сегодняшний день преступления в сфере компьютерной информации совершаются все чаще, так как работу с большим объемом данных мы не можем представить без современной техники. Однако, все еще не выработано эффективных методик расследования подобных видов преступлений, поэтому их

раскрываемость находится на низком уровне.

Одним из преступлений, входящих в главу 28 УК РФ, является неправомерный доступ к компьютерной информации (ст.272 УК РФ). Для начала обратимся к статистике.

Таблица. Статистика осужденных по ст.272 УК РФ [6].

	2019	**2020**	**2021**
Ст.272 ч.1	12	8	9
Ст.272 ч.2	16	12	13
Ст.272 ч.3	55	64	111
Ст.272 ч.4	2	0	0

Из приведенных данных видно, что в 2019 году всего было осуждено 85 человек, в 2020 – всего на одного человека меньше – 84, в 2021 наблюдается резкий рост – 133 человека. Также можно отметить, что наибольшее количество преступлений совершается по части третьей данной статьи – совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.

Рассмотрим основные проблемы, которые появляются при квалификации данного состава.

Первое, что хотелось бы выделить, это проблема толкования предмета преступления, предусмотренного ст.272 УК РФ. В части первой данной статьи указывается: неправомерный доступ к охраняемой законом компьютерной информации… Возникает вопрос: а что понимается под охраняемой законом информацией? В научной литературе сложились две противоположные точки зрения. Одни авторы считают, что под эту категорию попадает любая информация, к которой был получен доступ незаконно, против воли ее владельца. Другие уверены, что это информация, составляющая государственную и иную охраняемую законом тайну (налоговую, банковскую, врачебную, адвокатскую и т.д.). Вторая точка зрения является наиболее распространенной. К тому же, в методических рекомендациях, утвержденных

Генеральной прокуратурой РФ, четко написано: «Под охраняемой законом понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.)» [5, с. 85].

В силу расхождения мнений ученых судебная практика складывается неоднозначно. Как же следует квалифицировать незаконные деяния с информацией, имеющейся в открытом доступе?

Рассмотрим пример. Гражданин Анищенко, руководствуясь соображениями любопытства и проверки собственных навыков владения компьютерными программами, неправомерно запросил логин и пароль для входа на сайт на правах администратора и осуществил вход на сайт техникума. Пользуясь случаем, он удалил имеющуюся информацию, заменив ее графическим изображением черного флага с арабской вязью. Таким образом, Анищенко совершил неправомерный доступ к охраняемой законом компьютерной информации сайта и осуществил ее удаление и модификацию [3].

При постановлении приговора суды обращаются к Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также к Постановлениям Правительства РФ и некоторым ведомственным нормативным актам. Эти документы содержат положения о том, что общедоступная информация наряду с закрытой подлежит обязательной защите государством. Следовательно, она тоже попадает под сферу действия ст. 272 УК РФ.

В части второй ст.272 УК РФ установлена повышенная уголовная ответственность за деяния, перечисленные в части первой, если они повлекли причинение крупного ущерба или совершены из корыстной заинтересованности.

Гражданин П. заведомо знал о том, что его хотят уволить за прогулы, следовательно, прямой доступ к сетевой инфраструктуре организации ему будет недоступен. У него возник прямой умысел на неправомерный доступ к охраняемой законом компьютерной информации с целью ее последующего уничтожения. Так, используя свои навыки и умения в компьютерной сфере, с

помощью специальных программ П. получил доступ к охраняемой законом компьютерной информации и уничтожил программное обеспечение. Тем самым, работа серверов была приостановлена. Деяние гражданина П. повлекло причинение крупного ущерба на общую сумму 1 469 062 руб. 00 коп. [4].

Анализируя данный приговор Кировского районного суда, можно выявить такой квалифицирующий признак, как корыстная заинтересованность, о чем свидетельствует умысел П., направленный на уничтожение информации с целью получения выгоды или избавления от материальных затрат. Стоит отметить, в судебной практике данный квалифицирующий признак не рассматривается, либо же суды указывают отдельные предложения, как в рассматриваемом приговоре «осознавал, что в связи с его предстоящим увольнением прямой доступ к сетевой инфраструктуре вышеуказанной организации ему будет запрещен». Можно предположить, что данный квалифицирующий признак, как корыстный мотив не вменяется, так как не всегда удается на практике выявить и доказать корыстную заинтересованность лица.

Следующая проблема, которую хотелось бы выделить, это совокупность преступлений, предусмотренных ст.272 УК РФ с другими статьями, например, 158, 159, 275, 276 и др. К примеру, совокупность ст.272 и ст.158 УК РФ имеет место в тех случаях, когда преступник намерен совершить хищение денежных средств, незаконно получив перед этим доступ к необходимой ему информации [2, с. 405].

В апелляционном постановлении Верховного Суда Республики Татарстан по делу № 22-7630 от 01.11.16 г. решение суда первой инстанции было оставлено без изменения.

Граждане Г. и Б., действуя по предварительному сговору, при помощи специального оборудования и программного обеспечения негласно получали информацию с банкоматов путем ее копирования, затем расшифровывали ее, изготавливали дубликаты банковских карт и пользовались денежными средствами, содержащимися на этих картах, без согласия настоящих владельцев. Ново-Савиновский районный суд г. Казани квалифицировал действия лиц по пп.

«а», «в» ч. 2 ст. 158 УК РФ, ч. 3 ст. 272 УК РФ.

Верховный суд Республики Татарстан в ответ на поданную апелляционную жалобу в отношении Г. отметил, что «…Поскольку Г. … собирал сведения, составляющие банковскую тайну, путем неправомерного доступа к компьютерным сетям, его действия правильно квалифицированы по совокупности со статьей 272 УК РФ. В связи с тем, что полученная информация была в последующем использована для похищения денежных средств, действия Г. … правильно квалифицированы и по статье 158 УК РФ» [1].

Таким образом, судам следует помнить, если при совершении преступлений против собственности похищается, уничтожается или повреждается компьютерная техника, данное деяние будет квалифицировано по соответствующей статье УК РФ (158-168). Однако, если преступник овладевает компьютерной информацией без ведома ее владельца, содеянное не охватывается вышеуказанными составами преступления и подлежит квалификации дополнительно по ст. 272 УК РФ. В нашем случае банкомат будет являться только способом совершения преступления, умысел виновных был направлен на получение информации, содержащихся в этих аппаратах.

Библиографический список:

1. Апелляционное постановление Верховного Суда Республики Татарстан (Республика Татарстан) № 22-7630 от 01.11.16 по делу № 22-7630 // Официальный сайт Верховного суда Республики Татарстан: URL: http://vs.tat.sudrf.ru/modules.php?name=sdp2_cases#id=3_fb4207ece068e2a297901e67df4c44fc&shard=r16&from=p&r=%7B%22dateValue%22:%2201.11.2016%22%7D (Дата обращения: 04.07.2022).

2. Желтухина Е. В. Отдельные аспекты квалификации хищений в сети «интернет» и неправомерного доступа к компьютерной информации // Аллея науки. 2019. Т. 2. № 11. С. 404-407.

3. Приговор Волжского городского суда (Волгоградская область) № 1-1105/2016 от 17.11.2016 по делу № 1-1105/2016 // Судебные и нормативные акты

Российской Федерации: URL: https://sudact.ru/regular/doc/a8Mdo2yd0TLB/ (Дата обращения: 02.07.2022).

4. Приговор Кировского районного суда г. Хабаровска (Хабаровский край) № 1-3/2017 1-45/2016 от 23.03.2017 по делу № 1-3/2017 // Судебные и нормативные акты Российской Федерации: URL: https://sudact.ru/regular/doc/oHngqimjPHmz/ (Дата обращения: 03.07.2022).

5. Русскевич Е. А. О проблемах квалификации неправомерного доступа к компьютерной информации // Уголовное право. 2017. № 5. С. 85-91.

6. Статистика преступлений и наказаний в России // Электронный ресурс: URL: https://beta.dostoevsky.io/ru/ (Дата обращения: 02.07.2022).