УДК 343.2/.7

М. В. Ульянов
ведущий научный сотрудник
отдела Научно-исследовательского института
Университета прокуратуры Российской Федерации,
кандидат юридических наук

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: УГОЛОВНО-ПРАВОВЫЕ МЕРЫ ПРЕДУПРЕЖДЕНИЯ

Факты неправомерного распространения личной информации встречаются в правоприменительной деятельности как органов государственной власти, так и негосударственных структур, наделенных правом доступа к информации частного характера. Многочисленные факты утечек данных клиентов провайдеров, пользователей сайтов интернет-магазинов, служб доставки, образовательных порталов, интернет-ресурсов федеральных органов исполнительной власти актуализируют вопросы эффективности уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные гл. 28 Уголовного кодекса Российской Федерации (далее — УК).

С учетом того что нормы, предусматривающие уголовную ответственность за совершение преступлений в сфере компьютерной информации, направлены на предупреждение иных преступлений и правонарушений непреступного характера, некоторые исследователи относят их к преступлениям с двойной превенцией [1, с. 170].

Анализ судебной практики показывает, что на создание условий осуществления корыстных преступлений прежде всего направлены нормы, предусматривающие уголовную ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК) и создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).

Самой многочисленной группой осужденных по данным статьям являются работники коммерческих организаций (сотрудники офисов продаж, операторы связи и др.). Полученные незаконно персональные данные используются данной категорией непосредственно в целях совершения хищений либо передачи третьим лицам. Зачастую такие сотрудники выявляются службами безопасности организаций.

Повышенной степенью общественной опасности характеризуются преступления, совершаемые сотрудниками правоохранительных органов, имеющих доступ к соответствующим базам данным. Количество данной категории осужденных незначительно.

Еще одним преступлением, создающим условия для совершения хищений, является создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК).

Использование «вирусов» нередко осуществляется для обеспечения неправомерного доступа к вычислительным ресурсам с целью извлечения материальной выгоды, например, для взлома программного обеспечения и его использования в личных целях или реализации, майнинга криптовалют [2, с. 106–125].

Количественные показатели иных преступлений, составляющих главу 28 УК, значительно ниже по сравнению с показателями ст. 272 и 273 УК.

Диспозиции ст. 274 («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей») и ст. 274.1 («Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации») УК подвергаются определенной критике среди ученых [3, с. 393, 394; 4, с. 49–52].

Последняя на сегодняшний день ст. 274.2 УК, включенная в гл. 28 УК РФ, была введена Федеральным законом от 14 июля 2022 г. № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» [5]. Новая статья предусматривает ответственность за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования. Субъект преступления специальный — должностное лицо или индивидуальный предприниматель после его привлечения к административной ответственности по ч. 2 ст. 13.42 или ч. 2 ст. 13.42.1 Кодекса Российской Федерации об административных правонарушениях.

Принятие подобных изменений говорит о том, что законодателем осознается, что в условиях нарастания угроз информационной безопасности нормы, закрепленные в гл. 28 УК, нацелены на обеспечение уголовно-правовой охраны информационной среды, средств коммуникации и связи.

Как было указано, преступления в сфере компьютерной информации могут совершаться в целях нанесения ущерба национальной безопасности.

Не случайно был принят Федеральный закон от 14 июля 2022 г. № 266-ФЗ [6], которым вводится обязанность операторов незамедлительно информировать об инцидентах с принадлежащими им базами персональных данных уполномоченные органы власти, а также обеспечивать непрерывное

взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. За отказ предоставлять документы, подтверждающие, что хранение и обработка персональных данных российских пользователей осуществляются на территории Российской Федерации, Роскомнадзором составляются административные протоколы по ст. 13.11 Кодекса Российской Федерации об административных правонарушениях. Так, 28 июля 2022 г. Таганским районным судом г. Москвы в порядке административного судопроизводства оштрафованы иностранные компании Snap Inc. (1 млн рублей); Match Group, LLC (2 млн рублей); Hotels.com, LP. (1 млн рублей); Spotify AB (500 тыс. рублей); WhatsApp LLC (18 млн рублей за повторное нарушение требований о локализации).

Подытоживая изложенное, следует отметить, что нормы об ответственности за преступления в сфере компьютерной информации, осуществляя двойную превенцию, направлены не только на защиту компьютерной информации, но также на защиту собственности, интеллектуальной собственности, личных прав граждан, а также общественной безопасности.

Причем превентивный потенциал уголовно-правовых норм об ответственности за совершение неправомерного доступа к компьютерной информации (ст. 272 УК), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК) в большей степени нацелены на предупреждение хищений, нарушений тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, нарушений авторских и смежных прав, иных правонарушений, в том числе непреступного характера. В свою очередь нормы об ответственности за иные преступления в сфере компьютерной информации (ст. 274, 274.1 и 274.2 УК) прежде всего связаны с предупреждением преступлений против общественной безопасности.

Совершение преступлений в сфере компьютерной информации в некоторых случаях наносит ущерб национальным интересам Российской Федерации, так как способствует возникновению криминогенных условий, результатом которых среди прочего может стать совершение преступлений террористической направленности.

Преступления в сфере компьютерной информации обладают высокой латентностью. Наиболее действенной мерой, направленной на недопущение утечек персональных данных, является создание условий для совершенствования систем безопасности коммерческих организаций и органов государственной власти, имеющих доступ к ним.

Список основных источников

1. Фролов М. Д. Уголовно-правовое и криминологическое противодействие мошенничеству в сфере компьютерной информации : дис. ... канд. юрид. наук : 12.00.08. М., 2018. 211 с. Вернуться к статье

2. Русскевич Е. А., Малыгин И. И. Преступления, связанные с обращением криптовалют: особенности квалификации // Право. Журн. Высш. шк. экономики. 2021. № 3. С. 106–125. Вернуться к статье

3. Степанов-Егиянц В. Г. Совершение кражи и мошенничества с использованием компьютера или информационно-телекоммуникационных сетей // Риск: ресурсы, информация, снабжение, конкуренция. 2012. № 4. С. 393–396. Вернуться к статье

4. Кругликов Л. Л., Соловьев О. Г., Бражник С. Д. Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в системе экономической и информационной безопасности государства // Вестн. Ярослав. гос. ун-та им. П. Г. Демидова. Сер. Гуманитар. науки. 2019. № 4. С. 49–52. Вернуться к статье

5. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации : Федер. закон, 14 июля 2022 г., № 260-ФЗ // Российская газета. № 154–155. Июль 2022. Вернуться к статье

6. О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» : Федер. закон, 14 июля 2022 г., № 266-ФЗ // Российская газета. № 156–157. Июль 2022. Вернуться к статье