И. Р. Бегишев

ПРОБЛЕМЫ ОТВЕТСТВЕННОСТИ ЗА НЕЗАКОННЫЕ ДЕЙСТВИЯ С ИНФОРМАЦИЕЙ, ЗАВЕДОМО ДОБЫТОЙ ПРЕСТУПНЫМ ПУТЕМ

Информационный век высоких технологий немыслим без оперативного обмена информацией. Цифровая информация окружает нас повсюду: в работе за компьютером, при передаче данных в системах мобильной связи, при работе с использованием беспроводных технологий передачи данных, в сети Интернет и т. д. Порой цифровая информация является не только объектом преступных посягательств, но и объектом экономической деятельности.

По данным аналитического отчета компании InfoWatch, специализирующейся на защите конфиденциальной информации, в первом полугодии 2009 г. было установлено 413 инцидентов утечки информации из организаций: из них 64,2 % — из коммерческих организаций, 21,3 % — из государственных организаций, 10,4 % — из некоммерческих и образовательных организаций, 4,1 % — из неустановленных организаций. По видам этих утечек информации к умышленным утечкам отнесены 55,9 %, к случайным 39,0 %, к неустановленным 5,1 % всех утечек информации. По типу информации все утечки группируются следующим образом:

персональные данные — 87,2 %,

коммерческая тайна, ноу-хау — 2,9 %,

государственная и военная тайна — 2,2 %,

другая конфиденциальная информация — 6,8 %,

не установлено — 1,0 %

от числа всех зафиксированных утечек. Необходимо отметить, что данные о вышеупомянутых утечках включают все инциденты во всех странах мира, информация о которых была опубликована в СМИ, а также в блогах, веб-форумах и других сетевых ресурсах [1].

Ограничение оборота цифровой информации, заведомо добытой преступным путем, является ключевым фактором противодействия преступлениям в сфере высоких технологий и, несомненно, нуждается в уголовно-правовой защите.

Постоянные предложения приобрести различные (в большинстве своем ведомственные) базы данных свидетельствуют о том, что продажа конфиденциальных сведений о гражданах и юридических лицах стала отдельным видом бизнеса. Если появление очередной опубликованной базы для граждан является просто еще одним малоприятным фактом обнародования сведений об их частной жизни, то на некоторых предприятиях это может отрицательно повлиять на бизнес. Например, для оператора сотовой связи распространение базы биллинга может обернуться существенным оттоком абонентов к более «надежному» оператору-конкуренту. Поэтому оператору подчас экономически более выгодно найти «производителя», подготовившего украденную базу к продаже, и выкупить весь тираж. Но проблема перекрытия возможных утечек при этом остается весьма актуальной [2].

Существенным пробелом в Уголовном кодексе Российской Федерации (далее — УК РФ) является отсутствие в нем нормы, устанавливающей ответственность за приобретение или сбыт информации, заведомо добытой преступным путем.

Информацию обычно не признают имуществом, и поэтому манипуляции с ней не подлежат ответственности по ст. 175 УК РФ «Приобретение или сбыт имущества, заведомо добытого преступным путем», так как в ней под имуществом понимают те или иные материальные ценности, состоящие во владении какого-либо лица. Думается, что цифровая информация имеет определенную схожесть с некоторыми вещами с точки зрения их ценности. Однако между

ними имеется принципиальное различие: цифровую информацию, по сравнению, например, с драгоценным металлом или ценной бумагой, являющимися материальными ценностями, невозможно потрогать и ощутить, хотя носитель информации (например, компьютер), на котором находится цифровая информация, является материальной ценностью. Компьютер в этом случае будет являться предметом преступления, предусмотренного ст. 175 УК РФ.

Следует отметить, что помимо незаконных действий с цифровой информацией непоправимый ущерб гражданам и организациям могут нанести также и незаконные действия с документированной информацией. Например, торговля украденными платежными и другими документами, бизнес-планами и иными материалами может в итоге отрицательно повлиять на деловую репутацию физического или юридического лица, причинить ему ущерб. Бумага, на которой изложена информация, какой-либо ценности не имеет, а вот сама она ценность представляет. Ярким примером соответствующего деяния является следующее событие из зарубежной практики: конфиденциальная медицинская информация пациентов одного из дорогих частных госпиталей Великобритании была продана сыщикам, работавшим под прикрытием. Сотни документов, содержащих личную информацию о состоянии здоровья пациентов, их домашние адреса и даты рождения, предлагались по J4 за каждый [3].

Учитывая, что ст. 175 УК РФ не содержит указаний на такой предмет, как цифровая и документированная информация, и в связи с вышесказанным предлагаем установить ответственность за сбыт и приобретение цифровой и документированной информации, заведомо добытой преступным путем, и ввести соответствующую норму в УК РФ в следующей редакции:

Статья 272.1. Приобретение или сбыт охраняемой законом цифровой и документированной информации, заведомо добытой преступным путем, — наказывается ...

Квалифицирующим признаком приобретения и сбыта цифровой и документированной информации, заведомо добытой преступным путем, может быть совершение его организованной группой или лицом с использованием своего служебного положения, что довольно часто встречается на практике.

СПИСОК ЛИТЕРАТУРЫ:

1. Аналитический отчет «Глобальное исследование утечек. Первое полугодие 2009». URL: http://www.infowatch.ru/threats_and_risks/analytical_reports/2811 (дата обращения 08.11.2009).
2. Безопасность баз данных. Что, от кого и как надо защищать. URL: http://www.aladdin.ru/press-center/publications/publication5219.php?print=Y&ID=5219 (дата обращения 08.11.2009).
3. Великобритания: данные пациентов продаются на черном рынке. URL: http://www.dailymail.co.uk/news/article-1221186/Private-medical-records-sale-Harley-Street-clinic-patients-files-outsourced-input--end-black-market.html (дата обращения 08.11.2009).