На основании проведенного анализа Кодекса об административных правонарушениях РФ можно утверждать, что на сегодняшний день административное законодательство требует серьезных дополнений, в части дополнения кодекса рядом приведенных выше статей, которые помогут расширить профилактическую и превентивную роль действующего законодательства.

УДК 343.2

Бак. М.И. Горобец
Рук. И.В. Щепеткина
УГЛТУ, Екатеринбург

СУЩНОСТЬ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

На современном этапе развития технологий стало сложно представить себе наше общество без компьютеров, так как они стали важной частью в жизни людей: теперь досуг, работа и учеба большинства граждан нашей страны невозможны без использования компьютерной информации.

Безусловно, современные информационные технологии смогли вывести человечество на новый уровень. Благодаря им люди по всему миру могут развиваться и получать новые знания, не выходя из дома. Но есть люди, которые воспринимают компьютеры не только как источник информации, но и как возможность совершения преступлений.

Что же представляют собой преступления в данной сфере? Для изучения данного вопроса необходимо обратиться к самому определению компьютерной информации. Под данным определением, исходя из примечаний к статье 272 Уголовного кодекса Российской Федерации (УК РФ), следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Официального определения термина «преступление в сфере компьютерной информации» нет, но в основном мнения ученых сходятся в том, что такие преступления представляют собой запрещенные уголовным законом посягательства на безопасность в сфере использования компьютерной информации, которые при этом несут существенный вред или создают угрозу причинения такого вреда личности, обществу или государству.

В 2001 году в Будапеште была принята Конвенция Совета Европы о преступности в сфере компьютерной информации, в которой закрепили следующие группы компьютерных преступлений:

– правонарушения, связанные с использованием компьютерных средств;

– преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;

– правонарушения, связанные с нарушением авторского права и смежных прав;

– правонарушения, связанные с содержанием данных.

Глава 28 УК РФ устанавливает следующие виды преступлений в сфере компьютерной информации:

– неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

– создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);

– неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

Для наилучшего понимания сущности преступлений в сфере компьютерной информации следует назвать факторы, которые делают их опасным для общества явлением: во-первых, количество данных преступлений увеличилось; во-вторых, нет гарантий того, что вы от данных преступлений застрахованы.

В связи с массовым использованием компьютеров преступления, связанные с использованием компьютерной информации, стали представлять реальную угрозу. По данным сайта Генеральной прокуратуры РФ от 14 августа 2018 года, в 2017 году число преступлений в сфере информационно-телекоммуникационных технологий увеличилось с 65949 до 90587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4 % – это почти каждое 20-е преступление. При этом большинство таких преступлений приходится на преступления в сфере компьютерной информации, конкретно, на неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ) [1].

Не учитывая такие вещи, как пол, возраст и социальное положение, следует понимать, что любой человек может столкнуться с компьютерным преступлением. Само наличие у человека компьютера делает его потенциальной жертвой преступников. Во избежание этого необходимо принимать меры защиты. Наиболее массовыми считаются преступления на почве вредоносных программ и неправомерного доступа, поэтому стоит рассмотреть меры защиты от этих преступлений.

Аппаратно-программными средствами, которые обеспечивают защиту от неправомерного доступа, являются:

– системы идентификации и аутентификации пользователей;
– системы для шифрования дисковых данных;
– системы для шифрования данных, передаваемых по сетям;
– системы аутентификации электронных данных;
– средства для управления криптографическими ключами.

Обычным пользователям подойдут наиболее простые для применения меры защиты:

1) использование актуальных антивирусных программ и их регулярное обновление.

2) максимальная осторожность при переходе по сторонним ссылкам на различных сайтах;

3) использование программ от спама.

Важно понимать, что использование всех мер защиты не может обезопасить полностью, но может свести проблему к минимуму.

От данных преступлений уровень негативных последствий велик. Стоит понимать, что жертвой таких преступлений может оказаться не только обычный человек, но и крупная фирма, банк или даже государственная структура. К примеру, была совершена хакерская атака летом 2018 года на один из российских банков, в результате чего злоумышленники вывели 58 миллионов рублей с его корсчета в Центральном Банке РФ. В этом случае были затронуты права и интересы множества людей, работников банка и его вкладчиков.

Все эти преступления являются следствием глобализации и развития сетевых технологий, ведь именно это позволяет преступникам создавать большие сети для совершения преступлений.

В 2008 году наша страна подписала Соглашение о сотрудничестве государств СНГ в борьбе с преступлениями в сфере компьютерной информации. На наш взгляд, данное сотрудничество по борьбе с компьютерными преступлениями очень важно, ведь к наиболее эффективному результату можно прийти только совместными усилиями.

При расследовании таких преступлений у правоохранительных органов возникают затруднения. Выявление преступника, совершившего компьютерное преступление, для следствия очень сложно, поскольку здесь играет роль сама личность преступника, так как такие преступления, как правило, совершают профессионалы в данной сфере. Это высококвалифицированные программисты, IT-специалисты и др. Таких преступников сложно вычислить, ведь им хватает знаний, чтобы совершить преступление и при этом максимально остаться скрытными для следствия.

При условии, если даже будет найдено место, откуда было совершено преступление, все равно будет сложно найти преступника, ведь существует множество программ для шифрования, а также не исключено использование гаджетов, ему не принадлежащих. Кроме того, иногда не регистрируются дела, связанные с преступлением в сфере компьютерной информации. Проанализировав статистику преступлений с 2009 по 2019 год, мы пришли к выводу, что количество преступлений в сфере компьютерной информации, которые были выявлены и соответственно возбуждены уголовные дела, с каждым годом становится меньше. Около 20 % зарегистрированных уголовных дел прекращается на стадии предварительного расследования. В суд направляется чуть более 50 % уголовных дел [2].

Библиографический список

1. Новости Генеральной Прокуратуры России. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий. URL: http://genproc.gov.ru/smi/news/ genproc/ news-1431104/ (дата обращения 15.11.2019).

2. Евдокимов К.Н. Структура и состояние компьютерной преступности в Российской Федерации // Юридическая наука и правоохранительная практика. 2019. № 1 (35). С. 92.

УДК 336.74

Бак. К.Л. Иванов
Рук. И.В. Щепеткина
УГЛТУ, Екатеринбург

КРИПТОВАЛЮТА: ПРОБЛЕМЫ ЛЕГАЛИЗАЦИИ, РИСКИ И ПЕРСПЕКТИВЫ

На сегодняшний день в нашей стране правовой статус криптовалюты, операций с ней и ее налогообложение не определены, потому что методологическая и юридическая базы регулирования до сих пор отсутствуют. Что имеем в результате? А то, что компании, которые осуществляют криптовалютную деятельность, официально не зарегистрированы, непрогнозируемые действия органов государственной власти и контрагентов в отношениях с субъектами рынка криптовалюты создают препятствия проведению нормальной криптовалютной деятельности. В частности, это риски признания данной деятельности незаконной, проблемы с банковским обслуживанием, непризнание смарт-контрактов и тому подобное.