

Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

**Преступления в сфере компьютерной информации: проблематика и оценка целесообразности законодательных изменений**

**Научный руководитель – Каменева Анна Николаевна**

***Василихина Юлия Владимировна***

*Студент (магистр)*

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия

*E-mail: vasilihina7@gmail.com*

Развитие информационных технологий обусловило закрепление в 1996 году в Уголовном кодексе РФ составов преступлений в сфере компьютерной информации, обособленных главой 28. Первоначально в нее было включено три преступных посягательства. Позднее, в 2017 и 2022 годах глава была дополнена двумя составами.

Данная группа преступлений вызывала дискуссии с момента ее появления [1]. Спорные вопросы остаются не разрешенными и сейчас. Часть из них лежит в плоскости обоснованности существования специализированной главы, актуальности и полноты покрытия ею всех общественно-опасных деяний, которые в настоящее время могут совершаться с использованием компьютерных технологий и информации, часть – в области элементов состава преступлений, их содержания и особенностях их расследования. Первая группа подлежит рассмотрению далее.

Действующая редакция главы 28 Уголовного кодекса РФ содержит 5 составов преступлений в сфере компьютерной информации. К ним отнесены составы статей 272 - 274.2 УК РФ).

Однако с учетом активного развития и появления новых компьютерных и информационных технологий и отнесения к объекту преступления информации, обрабатываемой в компьютерной сети[5], данные составы не покрывают всю совокупность потенциальных общественно-опасных деяний, которые могут быть совершены с их использованием. Так, технологии искусственного интеллекта тесно вошли во все сферы жизни общества. При этом они благо и бремя одновременно, поскольку могут нести как пользу, так и вред и использоваться в преступных целях, увеличивая в силу своих характеристик общественную опасность, совершаемых преступных деяний или создавая поле для появления новых, еще не криминализованных составов преступлений.

Например, доктор юридических наук, выдающийся криминолог России В.С. Овчинский в своих трудах[6] выделяет следующие возможные направления использования систем искусственного интеллекта в преступных целях:

- 1) Дискредитация и внедрение вредоносных программ в платежные системы;
- 2) Противоправные деяния в сфере интеллектуальной собственности;
- 3) Посягательства на жизнь и здоровье человека;
- 4) Незаконные консолидация и распространение информации;
- 5) Экстремистская и террористическая деятельность (террористические акт, вандализм, выведение из строя объектов жизнеобеспечения и др.);
- 6) Криминальная 3D-печать (реализация контрафактного товара и др.).

Потенциально в таком качестве система искусственного интеллекта может применяться при совершении таких преступлений как мошенничество (ст. 159 УК РФ), вымогательство (ст. 163 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК

РФ), умышленное уничтожение или повреждение имущества (ст. 167 УК РФ), клевета (ст. 128.1 УК РФ), нарушение неприкосновенности частной жизни (ст. 137 УК РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ) и ряде других. Приведенный перечень не является исчерпывающим.

В следствии этого, границы главы 28 Уголовного кодекса РФ фактически подлежат размытию и утрачивают свою структурность. Наиболее релевантным в существующих обстоятельствах видится закрепление квалифицирующих признаков в отдельных составах преступлений по аналогии с п. «г» ч.3 ст. 158 УК РФ (кража с банковского счета, а равно в отношении электронных денежных средств), что позволит избежать путаницы в квалификации преступных деяний и разграничении смежных составов преступлений.

Существует проблематика и в терминологической, смысловой составляющей. На сегодняшний день формулировка преступления в сфере «компьютерной информации» не отвечает реалиям текущего законодательства. Наиболее корректным на наш взгляд является использование термина «информационные технологии» (ФЗ от 27.07.2006 №149). Эту позицию разделяет и ряд других исследователей[2,3,4]. О важности использования правильной терминологии с опорой на специализированные акты говорит и Постановление Пленума Верховного суда РФ "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"[8].

Помимо спорных положений в области законодательной техники существуют проблемы и в сфере правоприменительной практики. Согласно данным информационного банка «Судебная статистика РФ» данные категории преступлений не выделяются и судебная практика по ним не фиксируется, поскольку составляет единичный процент от общего числа уголовных дел. Хотя все же приговоры по пяти рассматриваемым статьям за период существования главы имеются. Данная ситуация нетипична, поскольку число посягательств с использованием информационных технологий прогрессирует, однако количество зафиксированных уменьшается. Во-первых, это демонстрирует латентный характер данной категории преступлений. Во-вторых, показывает сложность их раскрытия, что объясняется законодательной и практической непроработанностью структуры и содержание главы 28 УК РФ и ее норм.

Таким образом, следует вывод о том, что в Уголовный кодекс РФ в части норм, предусматривающих ответственность за преступления в сфере компьютерной информации, требуются изменения и являются целесообразными. Преобразования возможны по нескольким сценариям в комплексе:

- 1) структурные изменения в Уголовный кодекс РФ с полным пересмотром содержания норм главы 28 УК РФ и норм, иных составов, являющихся смежными составам глава 28 УК РФ;
- 2) уточнение терминологического аппарата и приведение его в соответствие со специальными законами;
- 3) расширение содержания предмета преступления для покрытие тех общественно-опасных деяний, которые порождаются развитием информационных технологий и для более активного законодательного реагирования на угрозы информационной безопасности.

### Источники и литература

- 1) Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: автореф. дис. ... канд. юрид. наук. Ижевск, 2002. С. 12.

- 2) Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. ... канд. юрид. наук. М., 2007. С. 12.
- 3) Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. ... канд. юрид. наук. Красноярск, 2002. С. 11.
- 4) Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: автореф. дис. ... канд. юрид. наук. Тамбов, 2007. С. 7 - 8.
- 5) Лавицкая М.И., Крапчатова И.Н. Структурно-содержательная характеристика главы 28 УК РФ: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации // Российский следователь. 2021. N 6. С. 35 - 41.
- 6) Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. М.: Норма, 2018. 351 с.
- 7) Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ//Собрание законодательства РФ", 17.06.1996, N 25, ст. 2954
- 8) Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37// "Российская газета", N 294, 28.12.2022