УДК 343

# *КВАЛИФИКАЦИЯ ДЕЙСТВИЙ ПО СОЗДАНИЮ, ИСПОЛЬЗОВАНИЮ И РАСПРОСТРАНЕНИЮ ВРЕДОНОСНЫХ ПРОГРАММ (СТ. 273 УК РФ): ОТГРАНИЧЕНИЕ ОТ СМЕЖНЫХ СОСТАВОВ*

***Самойлова А.С.*[1]**

*студент,*

*Белгородский государственный университет,*

*Белгород, Россия*

**Аннотация**

В статье рассматриваются проблемные аспекты квалификации преступлений, предусмотренных ст. 273 Уголовного кодекса Российской Федерации. Актуальность темы обусловлена стремительным развитием информационных технологий и ростом числа киберугроз, что требует от правоприменителя четкого понимания признаков состава данного преступления. Авторами уделяется внимание сложностям отграничения создания, использования и распространения вредоносных программ от смежных составов, таких как неправомерный доступ к компьютерной информации (ст. 272 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) и нарушение авторских прав (ст. 146 УК РФ).

**Ключевые слова:** вредоносные программы, ст. 273 УК РФ, компьютерная информация, квалификация преступлений, смежные составы, неправомерный доступ, судебная практика.

[1] Научный руководитель – Шумилина Оксана Сергеевна, доцент кафедры уголовного права и процесса, кандидат юридических наук, доцент, Белгородский государственный университет, Белгород, Россия

# *QUALIFICATION OF ACTIONS FOR THE CREATION, USE AND DISTRIBUTION OF MALWARE (ARTICLE 273 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION): SEPARATION FROM RELATED COMPOUNDS*

***Samoylova A.S.***
*student,*
*Belgorod State University,*
*Belgorod, Russia*

**Abstract**
The article discusses problematic aspects of the qualification of crimes under Article 273 of the Criminal Code of the Russian Federation. The relevance of the topic is due to the rapid development of information technology and the growing number of cyber threats, which requires a law enforcement officer to clearly understand the elements of this crime. The authors pay attention to the difficulties of distinguishing the creation, use and distribution of malware from related compounds, such as unauthorized access to computer information (art. 272 of the Criminal Code), fraud in the field of computer information (Article 159.6 of the Criminal Code) and copyright infringement (Article 146 of the Criminal Code).
**Keywords:** malware, Article 273 of the Criminal Code of the Russian Federation, computer information, qualification of crimes, related compounds, unlawful access, judicial practice.

В условиях цифровой трансформации всех сфер жизни общества особую опасность приобретают деяния, посягающие на безопасность компьютерной информации. Среди них центральное место занимает состав преступления, предусмотренный ст. 273 Уголовного кодекса РФ, который устанавливает ответственность за создание, использование и распространение вредоносных компьютерных программ. Как справедливо отмечает А.А. Энгельгардт,

применение данной статьи вызывает немало сложностей, а качество её применения зачастую зависит от активности правоохранительных органов, что порождает риск избирательного правоприменения [4].

Проблематика квалификации усугубляется наличием в уголовном законе ряда смежных составов, объективная сторона которых может пересекаться с действиями, описанными в ст. 273 УК РФ. Неправильное разграничение этих составов ведет к судебным ошибкам и нарушению принципа справедливости. На основе анализа теоретических источников и материалов судебной практики авторы данной работы определят основные критерии отграничения ст. 273 УК РФ от смежных составов преступлений.

Объективная сторона преступления, закрепленного в ст. 273 УК РФ, выражается в трех альтернативных формах: создание, использование и распространение компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты.

Как подчеркивает А.А. Энгельгардт, состав данного преступления является формальным. Для признания его оконченным не требуется наступления общественно опасных последствий; достаточно самого факта совершения действий, если они создавали угрозу их наступления [5]. Вредоносность программы определяется не её формальными характеристиками, а целевым назначением. В связи с этим И.А. Корепина указывает на проблему отсутствия в законе легального определения «вредоносной программы», что приводит к разночтениям в экспертной и судебной практике. Эксперты могут по-разному интерпретировать функционал программы, что напрямую влияет на квалификацию [2].

Наиболее тесная связь прослеживается между ст. 273 и ст. 272 УК РФ. Оба преступления посягают на безопасность компьютерной информации, однако имеют принципиальные различия.

Во-первых, разграничение проводится по предмету преступления. В ст. 272 УК РФ предметом выступает исключительно охраняемая законом компьютерная информация. Ст. 273 УК РФ охраняет любой вид информации (как охраняемой, так и неохраняемой), поскольку вредоносная программа может быть направлена на деструктивное воздействие на любые данные [1].

Во-вторых, ключевым является разграничение по объективной стороне. Ст. 272 УК РФ предусматривает совершение действий по неправомерному доступу к информации, которые влекут за собой конкретные материальные последствия (уничтожение, блокирование и т.д.). Ст. 273 УК РФ наказывает за сам факт создания инструмента для совершения таких действий (или иных манипуляций), независимо от того, был ли осуществлен неправомерный доступ и наступили ли последствия [1].

На практике возможна идеальная совокупность преступлений. Исследователи рассматривают пример из судебной практики, где лицо обвинялось одновременно по ст. 272 и ст. 273 УК РФ за использование вредоносной программы для кражи персональных данных. В одном из дел, рассмотренных Московским городским судом, суд пришел к выводу о конкуренции норм и квалифицировал действия только по ст. 272 УК РФ, что вызвало критику стороны обвинения [2]. В этой связи уточняется: если виновный создает вредоносную программу и с её же помощью осуществляет неправомерный доступ, содеянное должно квалифицироваться по совокупности преступлений, так как создание программы (ст. 273) и её использование для доступа и уничтожения информации (ст. 272) представляют собой два самостоятельных деяния [1].

Разграничение с мошенничеством проводится по объекту и предмету преступного посягательства. Ст. 159.6 УК РФ, как указывает А.А. Гончаров, относится к преступлениям против собственности. Компьютерная информация здесь выступает не предметом, а средством совершения хищения [3]. Предметом же выступают чужие денежные средства.

В отличие от этого, ст. 273 УК РФ посягает на общественную безопасность в сфере компьютерной информации. Если лицо создает вредоносную программу с целью последующего хищения денежных средств, но ещё не использовало её для этого, ответственность наступает по ч. 1 ст. 273 УК РФ за создание программы, а также как за приготовление к мошенничеству (ст. 159.6 УК РФ), если цель хищения будет доказана. Как отмечает А.А. Гончаров, сам по себе взлом паролей или создание вредоносного ПО для кражи реквизитов ещё не является хищением, а лишь создает условие для него [3].

А.З. Гобозов проводит четкую границу между данными составами. Основное различие лежит в объекте и потерпевшем. Ст. 146 УК РФ охраняет интеллектуальную собственность, и потерпевшим выступает автор или иной правообладатель. Ст. 272-274 УК РФ охраняют безопасность информационной среды. Потерпевшим может быть любое лицо [1].

Кроме того, для ст. 146 УК РФ обязательным признаком является причинение крупного ущерба, в то время как для основного состава ст. 273 УК РФ наступление последствий не требуется. Если лицо создало вредоносную программу для взлома защиты контрафактного программного обеспечения, его действия могут быть квалифицированы только по ст. 273 УК РФ, так как цели нарушить авторские права путем копирования и извлечения прибыли может и не быть. Однако, если взломщик копирует программу для дальнейшего использования, и это причиняет крупный ущерб правообладателю, содеянное требует квалификации по совокупности ст. 273 и ст. 146 УК РФ [1].

Комплексный анализ доктринальных источников и материалов судебной практики позволяет выявить ряд системных проблем, возникающих при квалификации деяний по ст. 273 УК РФ. В первую очередь, это проблема определения момента окончания преступления: правоприменители демонстрируют полярные подходы, одни суды считают преступление оконченным с момента создания исходного кода программы (даже существующего лишь на бумажном носителе), в то время как другие связывают

завершенность состава с фактическим запуском программы или её передачей третьим лицам, что подтверждается, в частности, приговором Ульяновского областного суда, где защита настаивала на исследовательском, а не вредоносном характере программы [2]. Второй ключевой проблемой выступает установление субъективной стороны, а именно прямого умысла и «заведомости» предназначения программы. Особую сложность здесь вызывают программы двойного назначения, которые могут легитимно использоваться для тестирования систем безопасности, но потенциально пригодны и для совершения атак; в отсутствие четких законодательных критериев доказывание преступной цели требует проведения сложных и дорогостоящих экспертиз, а также глубокого анализа всех обстоятельств дела [2]. Наконец, проблемой является терминологическая неопределенность: отсутствие в законе легальной дефиниции «вредоносной программы» создает широкий простор для судейского усмотрения и порождает риск экспертных ошибок, поскольку различные экспертные методики могут приводить к диаметрально противоположным выводам о функционале и предназначении одного и того же программного продукта [2].

В качестве путей решения обозначенных проблем исследователи предлагают комплекс мер: закрепление в уголовном законе либо в постановлении Пленума Верховного Суда РФ четкого определения «вредоносной программы», учитывающего не только её технические характеристики, но и целевую направленность; разработку и внедрение унифицированных методик проведения компьютерно-технических экспертиз для обеспечения единообразия экспертных заключений; а также принятие отдельного руководящего разъяснения высшей судебной инстанции, которое детализировало бы критерии разграничения ст. 273 УК РФ со смежными составами (ст. 272, 159.6, 146 УК РФ) и установило бы правила квалификации действий с программами двойного назначения и определения момента окончания данного преступления.

Таким образом, квалификация преступлений, связанных с вредоносными программами, представляет собой сложный процесс, требующий тщательного анализа всех элементов состава. Основными критериями отграничения ст. 273 УК РФ от смежных составов выступают объект преступления, характеристика предмета и содержание объективной стороны. При создании вредоносной программы с целью её дальнейшего использования для совершения иных преступлений (краж, мошенничеств, нарушений авторских прав) правоприменителю необходимо решать вопрос о совокупности содеянного.

**Библиографический список:**

1. Гобозов А.З. Проблема разграничения неправомерного доступа к охраняемой законом компьютерной информации от смежных составов преступления / А.З. Гобозов // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2020. – № 9. – С. 526–531.

2. Корепина И.А. Спорные вопросы квалификации преступлений, связанных с созданием, использованием и распространением вредоносных программ / И.А. Корепина // Вестник магистратуры. – 2025. – 5-4.

3. Гончаров А.А. Разграничение смежных составов хищения денежных средств с банковской карты / А.А. Гончаров // Наукосфера. – 2021. – № 4(2). – С. 302–306.

4. Энгельгардт А.А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации / А.А. Энгельгардт // Право. Журнал Высшей школы экономики. – 2014. – № 4. – С. 136–145.

5. Энгельгардт А.А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) / А.А. Энгельгардт // LEX RUSSICA. – 2014. – № 11. – С. 1318–1327.