

УДК 343.3/.7

Баландин Ф.Д.,
студент
Института прокуратуры
Московского
государственного
юридического университета
имени О.Е. Кутафина
(МГЮА),
г. Москва, Россия

Научный руководитель:
Пикуров Н.И.,
профессор кафедры
уголовного права Московского
государственного юридического
университета имени О.Е.
Кутафина (МГЮА), доктор
юридических наук, профессор

**ОБ ОТДЕЛЬНЫХ ПРОБЛЕМАХ КВАЛИФИКАЦИИ
ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ СТАТЬЁЙ 272
УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ**

В статье раскрываются проблемы квалификации преступлений, предусмотренных статьёй 272 Уголовного кодекса Российской Федерации. Проанализированы статистические сведения о совершённых преступлениях в сфере компьютерной информации на основе данных, представленных Генеральной прокуратурой Российской Федерации. На основе обобщения проблемных аспектов квалификации преступлений по статье 272 УК РФ с учетом исследования судебной практики сформулированы выводы, которые могут быть использованы в борьбе с неправомерным доступом к охраняемой законом компьютерной информации.

Ключевые слова: прокуратура; преступления; компьютерная информация; квалификация; неправомерный доступ; крупный ущерб; совершенствование; признаки.

Balandin F.D.,
student of the Institute of
Prosecutor's Office of the Moscow State
Law University named after O.E. Kutafin
(MGLA), Moscow, Russia

Supervisor:
Pikurov N.I.,
professor
of the Department of Criminal Law of the Moscow State Law
University named after O.E. Kutafin (MGLA),
Doctor of Law, Professor

ON CERTAIN PROBLEMS OF QUALIFYING CRIMES UNDER ARTICLE 272 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Abstract: The article reveals the problems of qualification of crimes under Article 272 of the Criminal Code of the Russian Federation. It analyzes statistical data on crimes committed in the field of computer information based on data provided by the General Prosecutor's Office of the Russian Federation. Based on a summary of the problematic aspects of the qualification of crimes under Article 272 of the Criminal Code of the Russian Federation, taking into account the analysis of judicial practice, the article formulates conclusions that can be used in the fight against unauthorized access to computer information protected by law.

Keywords: prosecutor's office; crimes; computer information; qualifications; unauthorized access; major damage; improvement; signs.

Неправомерный доступ к компьютерной информации, ответственность за который предусмотрена статьей 272 Уголовного кодекса РФ, является наиболее распространенным и вместе с тем одним из самых сложных для квалификации составов преступлений в сфере

компьютерной информации. Как справедливо отмечается в современной научной литературе, высокий уровень неопределенности в толковании понятий, связанных с неправомерным доступом к компьютерной информации, вполне закономерно вызывает отсутствие единообразной судебной и следственной практики применения данной статьи. Несмотря на активную разработку вопросов практического применения положений ст. 272 УК РФ в отечественной науке, многие аспекты квалификации данного посягательства остаются в настоящее время неразрешенными. В связи с этим анализ проблемных аспектов квалификации неправомерного доступа к компьютерной информации приобретает как теоретическое, так и прикладное значение, особенно в свете анализа судебной практики за последние три года.

Статистические данные свидетельствуют о значительном росте числа преступлений в сфере компьютерной информации. По данным Генеральной прокуратуры РФ, в 2022 году в России было зафиксировано 9308 преступлений в сфере компьютерной информации (рост на 45,6%), а в 2023 году правоохранительными органами уже зарегистрировано 37 101 подобное преступление (рост на 270%). При этом в суды направлены уголовные дела только по 1562 преступлениям (4,2%), а приостановлены по 26 095 преступлениям (70,4%). Столь низкий процент направления дел в суд во многом обусловлен сложностью квалификации и проблемами доказывания по данной категории уголовных дел.

Анализ судебной практики за 2019-2024 годы, проведенный экспертами на основе данных портала «Судебная статистика», показывает, что по статье 272 УК РФ судами вынесено наибольшее количество приговоров по сравнению с иными составами преступлений в сфере компьютерной информации. Количество приговоров с 2019 года значительно увеличилось: по части 1 статьи 272 УК РФ зафиксирован рост на 50%, а по квалифицированным составам (части 2-4) он составил почти

четырёхкратный рост. При этом суды рассматривают лишь около 1-2% от возбужденных по данным статьям уголовных дел, что отчасти объясняется длительными сроками следствия по таким делам.¹

Одной из наиболее значимых тенденций последних лет является изменение подхода правоохранительных органов к квалификации деяний, ранее относимых к иным статьям УК РФ. Как отмечают эксперты, статья 272 УК РФ стала инкриминироваться тем, чьи действия, по мнению следствия и судов, попадали под другие составы. Речь идет, в частности, о продаже «левых» сим-карт работниками салонов связи, которых ранее часто судили по статье 274.1 УК РФ. По ней же привлекали также медиков, оформлявших подложные сертификаты о вакцинации, и продавцов на заправочных станциях за мелкие махинации с бонусными системами. Однако в 2025 году в таких случаях злоумышленникам инкриминируют как раз статью 272 УК РФ. Например, именно по части 3 статьи 272 УК РФ было возбуждено уголовное дело в отношении трех сотрудников салона мобильной связи в Перми, которые ради выполнения плана продаж оформили большое количество сим-карт на персональные данные случайных лиц. На аналогичную квалификацию по ч. 3 ст. 272 УК РФ ориентируется и следственная практика в Иркутской области, где директор магазина электроники без ведома граждан оформляла SIM-карты на их имена для последующего использования в незаконном обналичивании денежных средств.

Объективная сторона преступления, предусмотренного ст. 272 УК РФ, характеризуется тремя обязательными элементами: деянием в виде неправомерного доступа к компьютерной информации; последствиями в виде уничтожения, блокирования, модификации либо копирования компьютерной информации; причинно-следственной связью между деянием и наступившими последствиями. Каждый из указанных элементов

¹ Портал «Судебная статистика», данные о количестве приговоров по ст. 272 УК РФ за 2019–2024 годы.

порождает в правоприменительной практике самостоятельные проблемы квалификации.

Первая группа проблем связана с определением понятия «неправомерный доступ». Легальное определение данного термина в уголовном законе отсутствует, что вынуждает правоприменителя обращаться к доктринальным толкованиям и разъяснениям Пленума Верховного Суда РФ. Как разъясняет Пленум Верховного Суда РФ в Постановлении от 15 декабря 2022 г. № 37, под неправомерным доступом понимаются совершение действий, направленных на получение возможности ознакомления, обработки, копирования, модификации либо уничтожения компьютерной информации в отсутствие на то права у лица, в том числе с преодолением средств защиты.

В судебной практике встречаются примеры неоднозначного толкования признака неправомерности доступа. Показательным в этом отношении является дело, рассмотренное Судебной коллегией по уголовным делам Верховного Суда РФ (Кассационное определение от 3 апреля 2024 г. по делу № 1-226/2021). Осужденный был признан виновным в неправомерном доступе к компьютерной информации в связи с нарушением условий лицензионного соглашения при использовании игровых консолей. Защита настаивала на том, что лицензионное соглашение не было доведено до пользователя, поскольку консоли приобретались без лицензионного системного программного обеспечения, а суд фактически установил нарушение не уголовного, а авторского права. Адвокат в кассационной жалобе утверждал, что суд, давая толкование определений «неправомерного доступа» и «компьютерной информации», сослался на взаимоисключающие правовые нормы и неверно применил нормы гражданского законодательства при определении правового режима неправомерного доступа к компьютерной информации. Данный пример иллюстрирует острую дискуссию о границах уголовно-правового понятия

«неправомерный доступ» и его соотношении с гражданско-правовыми категориями.

Вторая группа сложностей при квалификации касается оценки последствий неправомерного доступа. Законодатель выделяет четыре варианта негативных изменений компьютерной информации: ее уничтожение, блокирование, видоизменение либо создание копии. Каждое из указанных понятий является оценочным, что порождает неединообразие судебной практики. В качестве иллюстрации можно привести одно из дел, где суд усмотрел в действиях подсудимого признаки модификации информации с применением специального программного обеспечения, предназначенного для обхода средств защиты. В то же время сторона защиты, ссылаясь на заключение эксперта, утверждала, что использованные приложения в принципе не способны привести к подобным последствиям, а сама система защиты была отключена иными способами. Данный случай наглядно демонстрирует, насколько сложным может быть установление причинно-следственной связи между применением вредоносного программного обеспечения и наступившей модификацией данных.

Третья группа проблем связана с субъективной стороной деяния и наличием квалифицирующих признаков. Практике известны примеры осуждения лиц за совершение неправомерного доступа из корыстных побуждений. В том же деле один из эпизодов был квалифицирован именно по данному признаку. Кроме того, эксперты отмечают, что в последние годы нормы главы 28 УК РФ, включая статью 272, все чаще применяются в совокупности с традиционными составами, прежде всего с мошенничеством. Так, жителю Челябинска вменяли одновременно неправомерный доступ и мошенничество за то, что он оформлял кредиты на посторонних граждан, получая их личные данные через взломанные аккаунты на интернет-сервисах.

Четвертая группа проблем касается судебной практики назначения наказания. Статистика последних лет свидетельствует, что суды крайне редко приговаривают виновных по статье 272 УК РФ к реальному лишению свободы. Согласно исследованию, проведенному одной из профильных компаний, лишь 5% дел в сфере информационной безопасности завершаются реальными сроками. Гораздо чаще назначаются штрафы, условные меры либо запрет на занятие определенных должностей. В 2023 году в перечень возможных наказаний была включена конфискация имущества, однако на сегодняшний день сведений о ее применении не имеется. Приговоры с реальной изоляцией от общества хотя и стали выноситься с 2021 года (ранее такие случаи отсутствовали), но их доля остается незначительной и демонстрирует неустойчивую динамику. Примечательно, что удельный вес условных сроков и штрафов, преобладавших в 2019-2021 годах, заметно снизился, тогда как суды стали активнее применять такие альтернативные меры, как ограничение свободы, обязательные или исправительные работы. В упомянутом деле подсудимому по части 2 статьи 272 УК РФ было назначено наказание в виде одного года ограничения свободы, а при совокупности преступлений — двух лет ограничения свободы с дополнительным штрафом.

Пятая группа проблем связана с отграничением состава, предусмотренного статьей 272 УК РФ, от смежных составов и административных правонарушений. Ключевое значение здесь имеет разграничение с созданием и применением вредоносных программ по статье 273 УК РФ. Судебная практика нередко идет по пути одновременного осуждения лица по нескольким эпизодам обеих статей. В уже рассмотренном деле подсудимый был признан виновным по четырем эпизодам, подпадающим под части первую и вторую статьи 272 УК РФ, а также по трем эпизодам, квалифицированным по частям первой и второй

статьи 273 УК РФ. При этом апелляционная инстанция освободила его от штрафа по первому составу в связи с истечением сроков давности.

Не менее важно различать неправомерный доступ (статья 272) и нарушение правил эксплуатации средств хранения и обработки компьютерной информации (статья 274). Основным критерий здесь - субъект преступления. По статье 274 ответственность несет лицо, имеющее законный доступ к информации, но нарушившее правила ее эксплуатации. По статье 272 — лицо, которое такого права не имело либо превысило его допустимые пределы.

Обобщая анализ проблемных аспектов квалификации преступлений по статье 272 УК РФ с учетом судебной практики последних трех лет, можно сформулировать ряд выводов.

Главные сложности квалификации обусловлены неопределенностью содержания понятия «неправомерный доступ» (что ярко проявилось в деле, где защита настаивала на гражданско-правовом, а не уголовном характере нарушения), оценочным характером последствий, трудностями доказывания причинно-следственной связи в цифровой среде, а также необходимостью разграничения умысла и неосторожности при наступлении вредных последствий.

Квалифицирующие признаки - корыстная заинтересованность, крупный ущерб, использование служебного положения - также вызывают сложности в правоприменении. Статистика свидетельствует, что при резком росте регистрируемых преступлений (в 2023 году прирост составил 270%) до суда доходит лишь незначительная часть дел (около 4,2%), что говорит о серьезных проблемах с раскрываемостью и расследованием данной категории уголовных дел.

Судебная практика по статье 272 УК РФ отличается преимущественно мягким подходом: реальное лишение свободы

назначается только в 5% случаев, преобладают ограничение свободы, штрафы и условные меры.

В целях совершенствования правоприменения, на наш взгляд, представляется целесообразным выработать единые подходы к толкованию категории «неправомерный доступ», четко отграничив его от нарушений авторского права, а также разработать унифицированную методику расчета крупного ущерба. Выявленные проблемы будут учтены при последующем анализе квалификации преступлений по статье 273 УК РФ и рассмотрении совокупности компьютерных преступлений с посягательствами на собственность.

Литература/ использованные источники:

1. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 года.
2. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
3. Федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 26 июня 2026 года) «Об информации, информационных технологиях и о защите информации» // Российская газета. – 2026. - 01 июля 2026 года. - № 141–142.
4. Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание Законодательства РФ от 5 ноября 2012 года. № 45 ст. 6257.
5. Постановление Пленума Верховного Суда РФ от 15 декабря 2022 года № 37 «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"» // Российская газета. – 2022. – 28 декабря. – № 294.
6. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 года) // Совет Европы. Документ зарегистрирован в Европейской серии договоров (European Treaty Series, ETS) под номером ETS № 185.