DOI 10.37882/2223-2974.2025.03.20

# КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ: ПРОБЛЕМЫ ТОЛКОВАНИЯ И КВАЛИФИКАЦИИ

## COMPUTER INFORMATION IN CRIMINAL LEGISLATION: PROBLEMS OF INTERPRETATION AND QUALIFICATION

***V. Pekareva***
***N. Polischuk***

*Summary*. The direct object of criminal legal protection provided for by Article 272 of the Criminal Code of the Russian Federation are public relations related to the lawful access, creation, storage, modification, use of computer information by its creator, as well as its consumption by other persons. This crime in the sphere of computer information is characterised by a high degree of prevalence. This article presents a critical analysis of the criminal law norm in question in the light of modern trends. Particular attention is paid to the problem of compliance of the used legal categories with current technical realities. In order to clarify the content of the concept of «computer information» and justify the need for its actualisation in criminal legislation, the author's interpretation of the term is proposed, based on scientific research in the field of law, practical experience and analysis of technical features.

*Keywords*: unlawful access to computer information, criminal law, computer information offences, cybercrime, computer information, data, interpretation, unauthorised access.

***Пекарева Виктория Владимировна***
*Академия права и управления ФСИН России, г. Рязань*
*viktoria.pekareva@yandex.ru*
***Полищук Николай Иванович***
*доктор юридических наук, профессор,*
*Академия права и управления ФСИН России г. Рязань*
*nik-polishchuk@yandex.ru*

*Аннотация*. Непосредственным объектом уголовно-правовой охраны, предусмотренной статьёй 272 Уголовного кодекса Российской Федерации, выступают общественные отношения, связанные с правомерным доступом, созданием, хранением, изменением, использованием компьютерной информации её создателем, а также её потреблением иными лицами. Данное преступление в сфере компьютерной информации характеризуется высокой степенью распространённости. В настоящей статье представлен критический анализ рассматриваемой уголовно-правовой нормы в свете современных тенденций. Особое внимание уделяется проблеме соответствия используемых правовых категорий актуальным техническим реалиям. С целью уточнения содержания понятия «компьютерная информация» и обоснования необходимости его актуализации в уголовном законодательстве предлагается авторская интерпретация данного термина, базирующаяся на научных исследованиях в области права, практическом опыте и анализе технических особенностей.

*Ключевые слова*: неправомерный доступ к компьютерной информации, уголовное законодательство, преступления в сфере компьютерной информации, киберпреступления, компьютерная информация, данные, толкование, несанкционированное ознакомление.

Исследование правоприменительной практики подразумевает единообразное и последовательное толкование, конкретизацию и реализацию норм уголовного права правоохранительными органами. В.Н. Карташов поддерживает данную позицию, характеризуя правоприменительную практику как юридически персонифицированное и подзаконное преобразование социальной действительности, осуществляемое посредством государственной власти, и представляющее собой совокупность правоприменительной деятельности и вытекающего из нее опыта. Анализ применения норм, в частности таких, которые предусматривают ответственность за преступления в сфере компьютерной информации, позволяет выявить проблемные области, требующие дальнейшего уточнения или изменения правовых предписаний. Регулярное и своевременное обновление уголовного законодательства, особенно в сфере противодействия преступлениям в сфере компьютерной информации, является необходимым условием для их эффективного функционирования. Рассмотрим с пониманием и вниманием к деталям проблемы этой сферы и предложим пути к их эффективному решению.

Сущность состава преступления, предусматривающего наступление уголовной ответственности по ст. 272 УК РФ, заключается в несанкционированном доступе к защищенным данным, что может вести к нежелательным последствиям в виде уничтожения, блокирования, модификации или копирования информации, находящейся под государственной охраной или же распространяемой в сети Интернет и защищаемой ее владельцем.

Информация обладает разноплановым содержанием. По мнению Овчинского А.С., её можно представить в природной и общественной жизни, в технической сфере, где она возникает в реакциях на воздействие, фиксируется, накапливается и передается на естественных

и искусственных носителях (ресурсная), отражает окружающую реальность (фоновая)[7].

Не обращаясь к узкому варианту при толковании, можно отметить, что данная категория отвечает за данные, сопровождающиеся смысловой нагрузкой, помещенной в некоторый контекст; за сведения, как-либо оцениваемые приёмником. Как правило, получение информации связывают с уменьшением неопределенности существующего выбора; ответ на какой-либо заданный либо подразумеваемый вопрос [5]. Однако для цифровой среды и противоправных в ней деяний нас интересует этимологическое представление информации через кодирование, то есть через числовое выражение посредством присвоения символьным данным уникального двоичного кода, состоящего из комбинации. Емкое понятие информации определяется Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» — сведения (сообщения, данные) независимо от формы их представления. Более конкретизированную, но с широким охватом дефиницию можно встретить в интересующем нас уголовном составе, а именно в примечании к ст. 272 УК РФ. Законодатель обозначил одну из форм всего семантического и практического выражения. Под этим термином подразумеваются данные или сообщения, которые представлены в виде электронных сигналов и не зависят от способов их хранения, обработки или передачи.

В Постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. №37 обозначено, как и где находятся данные. Они могут быть размещены внутри памяти компьютеров и других цифровых устройств или сохранены на различных типах внешних электронных носителей (жесткие диски, USB-накопители и подобные устройства, в формате, который может быть обработан этими устройствами). Кроме того, данные могут передаваться через каналы электросвязи (например, локальные сети (LAN), широкополосные сети (WAN), Интернет или через беспроводные технологии, а именно Wi-Fi и Bluetooth). В постановлении конкретизировано, что подобной информацией может считаться государственная, коммерческая, служебная, личная, семейная или иная тайна, включая персональные данные. Также под защитой находятся сведения, которые владелец обеспечил охраной специальными средствами, чтобы никто не мог их испортить или получить доступ без разрешения. Это также имеет последствия для неоднозначности этимологии дефиниции.

При исследовании практики применения уголовного закона можно заметить две стороны определения в уголовных делах сущности компьютерной информации. Одна из них — критерий содержания, другая — установление владельцем особого порядка работы с целью обеспечения сохранности и ограничения доступа. В практической области применяются оба критерия в зависимости от конкретного дела и статьи. Например, информацию по смыслу ч. 1 ст. 272 УК РФ требуется считать охраняемой законом как по критерию ее содержания (данные, для которых законом установлен специальный режим правовой защиты, ограничен доступ, существуют условия отнесения к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение), так и по критерию обеспечения охраны этой информации ее обладателем с целью сохранности и (или) ограничения доступа к ней.

Стоит обозначить, что определение «компьютерная информация» в уголовном законодательстве, введенное изменениями УК РФ от 7 декабря 2011 г., не в полной мере отражает сущность информации в цифровом виде, ограничиваясь лишь ее связью с процессами, происходящими в электронно-вычислительных машинах (ЭВМ) и компьютерных сетях. Существующая формулировка ведет к ошибочному толкованию, что в большинстве случаев влечет к неоднородному характеру правоприменительной деятельности. Чтобы учесть широкий спектр потенциальных преступлений, нужно сделать акцент на инновационных составляющих. В. Быков и В. Черкасов отмечают, что развитие науки и техники предполагает появление новых средств хранения, обработки и передачи информации, следовательно, корректировка закона на постоянной основе неизбежна [1, с. 38]. Таким образом, оправданы нюансы, связанные с волоконно-оптическими каналами и различными устройствами смешанного назначения, включая облачные типы. Вопросы вызывает и форма, в которой представлена информация — электрический сигнал. Законодатель не учёл, что она может передаваться не только посредством электрических сигналов [2], как справедливо, обращает внимание А.В. Верещагина. Аналогичную позицию можно встретить в научных трудах Дворецкого М.Ю. [3]. Передача данных по оптоволоконному кабелю, основанная на световых сигналах, не является электронной по своей природе. Информация преобразуется в электронную форму только при обработке компьютером. Аналогично, передача данных по Wi-Fi использует радиоволны, которые преобразуются оконечными устройствами в электрические сигналы. Волны распространяются в пространстве и принимаются приемником, который преобразует их обратно в электрические сигналы, понятные электронным устройствам. Важно отметить, что сам процесс передачи информации по воздуху или по оптоволокну происходит без участия электронов как носителей информации в среде передачи. На практике возможен незаконный перехват радио- и световых сигналов, не являющихся электронными сигналами в процессе их передачи. Компьютерная информация

на магнитных носителях (например, банковские расчетные карты), CD, DVD-дисках также не является информацией, представленной в форме электрических сигналов. При описании не были затронуты сферы нанотехнологий, искусственного интеллекта, биометрии, где определение формы обработки или представления информации как компьютерной не сходится с существующей дефиницией в уголовном законодательстве в принципе.

Не исключено, что законодатель ориентировался исключительно на понятии дискретных сигналов. Однако из сказанного выше становится очевидным, что уголовно-правовая охрана «компьютерной информации», хранение и передача которой основаны на неэлектрических принципах, не предусмотрена.

Имеет смысл отметить, что понятие было введено, прежде всего, для целей уголовного права, в частности для составов преступлений главы 28 УК РФ. Формулировка нуждается в изменении, что можно реализовать двумя способами. Во-первых, из примечания ст. 272 УК РФ исключить термин «компьютерная информация», поскольку его содержание игнорирует технические аспекты. Возможный отрицательный опыт также может подвергнуться дискуссии, как и существующее определение, однако примером обратной ситуации при отсутствии законодательно закрепленных дефиниций технического характера — свидетельство положительных тенденций в правоприменительной деятельности в Китае, ведь в стране акцент в большей степени делается на регламентации мер и средств защиты, чем на толковании и уяснении. Во-вторых, можно рассмотреть возможность совершенствования сущности определения. В настоящее время предпочтение отдается второму варианту, так как в судебной практике при вынесении приговоров нередко ссылаются на содержание термина «компьютерная информация». В этом контексте важно учитывать, что правильное понимание и верная интерпретация термина «компьютерная информация» могут в совокупности существенно повлиять на правоприменительную практику и, соответственно, на защиту прав граждан. Необходимость адаптации законодательства к быстро изменяющимся техническим условиям становится все более актуальной проблемой.

Предлагаем следующую формулировку «компьютерная информация» в ст. 272 УК РФ, сущность которой исключает слова «представленные в форме электрических сигналов»[10] и оправдывает главную цель — ее разграничение от всех иных форм представления: «под компьютерной информацией понимаются пригодные цифровые данные вне зависимости от их формы представления, хранения, обработки и передачи». Это означает, что она может быть представлена в виде кода, текста, алгоритма, графиков, звука, видео и других цифровых форм. Также имеет возможность храниться на различных носителях, таких как жесткие диски, твердотельные накопители (SSD), оптические диски, флэш-память или в облачных хранилищах.

Это не делает формулировку тождественной той, которая закреплена в ст.2 Федерального закона от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» №149-ФЗ, поскольку признак цифровой принадлежности и технической привязки к «данным», связывают с информационными сетями и компьютерной системой. Соответствовать современной действительности является обязательным условием для уголовно-правовой охраны несанкционированного доступа такого типа информации. В защиту позиции обратиться стоит к взглядам российских ученых А.Ф. Мицкевича и А.В. Суслопарова — сторонников функциональной концепции информации касаемо компьютерных преступлений. Они полагают, что вместо термина «информация» в тексте уголовного закона желательно употреблять «данные».

Если сделать ссылку на апелляционное постановление Липецкого областного суда от 23 мая 2024 г. по делу №22-527/2024, где приводятся рассуждения о примечании к ст. 272 УК РФ, то можно обнаружить, что компьютерная информация и средство ее хранения это два независимых друг от друга различных предмета, и преступным является посягательство именно на компьютерную информацию, помещенную в средство хранения, но не являющуюся составной неотъемлемой частью этого средства хранения, о чем прямо сказано в примечании. Обработка такой информации возможна с помощью различных программных приложений, алгоритмов вычислительных процессов, которые могут включать в себя операции ввода, вывода, кодирования, шифрования, компрессии, анализа и синтеза данных [8].

Передача компьютерной информации может происходить через различные сетевые технологии, включая локальные сети (LAN), глобальные (например, Интернет), беспроводные сети (Wi-Fi, Bluetooth), а также через другие средства коммуникации, включая спутниковые и мобильные сети.

Измененная формулировка дефиниции, защищаемая в данной работе, также оправдывается новеллой законодательства в качестве специальной нормы по отношению к ст. 272 УК РФ. Согласно Федеральному закону от 30 ноября 2024 г. №421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» была дополнена глава 28 УК РФ и установлена уголовная ответственность за незаконное использование и (или) передачу, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно за создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных

хранения и (или) распространения. На первый взгляд, впечатление о подмене и смешивании понятий «персональные данные» и «компьютерная информация» с технической и правовой сторон, что на данный момент является очевидным, но в целях реализации целей уголовного закона отдача предпочтения данной формулировке не будет ошибкой, поскольку этимология использованной дефиниции законодателем охватывает две категории в принципе. Разбор характеристики «компьютерной информации, содержащей персональные данные», сводится прямо или косвенно к сведениям, относящимся к конкретному физическому лицу. Они, в свою очередь, представлены в форме электрических сигналов независимо от средств их хранения, обработки и передачи в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах либо на любых внешних электронных носителях (дисках, в том числе жестких накопителях, флеш-картах и т.п.), в форме, доступной восприятию компьютерным устройствам, и (или) передаваться по каналам электрической связи. В текущий момент это складывается из учета в совокупности таких правовых понятий как компьютерная информация, которая содержится в примечании к статье 272 УК РФ, так и персональные данные из Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных». Нужно понимать, чтобы избежать спорных моментов и излишних привязок к «электронным сигналам», необходимо прибегнуть к актуализации понятия «компьютерная информация» в примечании к ст. 272 УК РФ.

Также уголовно-правовая норма не должна ограничиваться одной вариацией и подразумевать наступление ответственности за вторжение в компьютерную информационную систему, ознакомление, получение данных из нее, предоставление доступа, а не только за обязательное наступление последствий в качестве блокирования, уничтожения, копирования или модификации. Усовершенствовать и одновременно ужесточить содержание ст. 272 УК РФ можно дополнением диспозиции «ознакомлением информации без имеющегося на это права независимо от вредоносных последствий». Подобное существует в Китае. Крайне важно уточнить юридические рамки и закрепить «несанкционированное ознакомление» как отдельное правонарушение. Несомненно, в продолжении защиты приведенной позиции, стоит отметить позицию М.А. Ефремовой, что уголовной ответственности лицо должно подлежать как в случае неправомерного доступа-состояния, так и в случае неправомерного доступа-процесса [4].

Таким образом, при анализе ст. 272 УК РФ приводятся рекомендации о совершенствовании примечания в плане изменения содержании дефиниции «компьютерная информация», что будет способствовать устранению существующих противоречий. Новизна заключается не только в актуальности выбранной темы, но и в практических задачах, с которыми сталкиваются правоприменители. В работе были представлены, как одним из факторов противодействия преступлениям в области компьютерной информации, несколько обоснованных предложений, которые ранее в полной мере не формулировались в подобных исследованиях, направленных на улучшение уголовно-правовых норм.

ЛИТЕРАТУРА


1. Быков В., Черкасов В. Понятие компьютерной информации как объекта преступлений // Законность. — 2013. — №12 (950). — С. 37–40.
2. Верещагина А.В. К вопросу о предмете неправомерного доступа к компьютерной информации / А.В. Верещагина // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. — 2020. — Т. 12, № 2. — С. 103–117. — DOI 10.24866/VVSU/2073-3984/2020-2/103-117. — EDN IGROKB.
3. Дворецкий М.Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 Уголовного кодекса РФ. Вестник ТГУ. 2013. № 12. С.527–532.
4. Ефремова М.А. Ответственность за неправомерный доступ к компьютерной информации по действующему уголовному законодательству // Вестник Казанского юридического института МВД России. 2012. №8.
5. Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву //Пробелы в российском законодательстве. 2010 г. №2.
6. Лысов, А.А. Гистерезис понятия «компьютерная информация» в уголовном законодательстве Российской Федерации / А.А. Лысов, А.В. Яковлев, А. Л. Клочкова // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. — 2022. — № 1(140). — С. 132–135. — EDN DCQCEQ.
7. Овчинский А.С. Информация в мире цифровых данных // Криминологический журнал. 2023. №3. URL: https://cyberleninka.ru/article/n/informatsiya-v-mire-tsifrovyh-dannyh (дата обращения: 23.01.2025).
8. Чернякова А.В. Понятие и уголовно-правовое значение компьютерной информации / А.В. Чернякова // Право и государство: теория и практика. — 2019. — № 11(179). — С. 224–226. — EDN GDZEKR.



Журнал «Современная наука: актуальные проблемы теории и практики»