

УДК 34.01

СЫЧЕВ Евгений Анатольевич,
кандидат юридических наук, доцент, доцент кафедры административной деятельности и организации деятельности ГИБДД Краснодарского университета МВД России, Краснодар, Россия
zoya-dmitrieva@yandex.ru;

SYCHIOV Evgueny Anatolyevich,
Candidate for Doctorate in Law, Associate Prof., Chair of Administration and State Inspection on Road Traffic Security (SIRTS) Operation Arrangement, Krasnodar University under Ministry of Interior of Russia.
zoya-dmitrieva@yandex.ru;

АЛЕСКЕРОВ Вагиф Исмаилович,
кандидат юридических наук, доцент, профессор кафедры оперативно-технических мероприятий органов внутренних дел Всероссийского института повышения квалификации сотрудников МВД России, Москва, Россия

ALESKEROV Vagif Ismailovich,
Candidate for Doctorate in Law, Associate Prof., Chair of Task-Related Procedural Measures by interior affairs bodies, All-Russia Institute of Advanced Vocational Training for Russian MIA officers, Moscow, Russia

КОЛОКОЛЬЧИКОВА Ольга Николаевна,
старший преподаватель кафедры оперативно-технических мероприятий органов внутренних дел Всероссийского института повышения квалификации сотрудников МВД России, Москва, Россия

KOLOKOLCHIKOVA Olga Nikolaevna,
Senior Lecturer, Chair of Task-Related Procedural Measures by interior affairs bodies, All-Russia Institute of Advanced Vocational Training for Russian MIA officers
Moscow, Russia

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ, КАК РАЗНОВИДНОСТЬ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

CRIMES COMMITTED IN TELECOMMUNICATION NETWORKS BEING A KIND OF CRIME IN THE DOMAIN OF COMPUTER-PROCESSED INFORMATION

Статья посвящена анализу норм различных отраслей прав, в частности информационной сфере, одной из наиболее динамичных и быстро развивающихся сфер общественных отношений, которая нуждается в адекватном правовом регулировании.

This paper dealt with exploration of standards from various legislation domains and namely in the domain of information, one of the most dynamic and rapidly advanced fields of public relations, which requires an adequate legal regulation.

Ключевые слова: преступления, компьютерная информация, компьютерные преступления, телекоммуникационные сети, закон, анализ, Уголовный кодекс.

Key words: crimes, computer-processed data/information, cybercrime, telecommunication networks, the Act, review, the Criminal Processing Code.

Преступления в сфере *компьютерной информации* являются новеллами в отечественном уголовном законодательстве. Необходимость установления уголовной ответственности за причинение вреда в связи с незаконным использованием компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности современного общества. Однако, к сожалению, до настоящего времени, во многих организациях, предприятиях, учреждениях и отраслях народного хозяйства по сравнению с информацией, зафиксированной на бумажных носителях[1], компьютерная информация остается наиболее уязвимой.

Анализ положений действующего Уголовного кодекса РФ позволяет сделать вывод о том, что законодатель в гл. 28 «Преступления в сфере компьютерной информации» ввел ряд понятий, не содержащихся ранее не только в понятийно-терминологическом аппарате уголовного права, но и в «информационном» законодательстве, так как ранее не было практических наработок и теоретических рекомендаций по раскрытию и расследованию преступлений в этой сфере. В целях своевременного документирования преступной деятельности данного вида преступлений и получения необходимой доказательной базы в отношении лиц, их совершивших, в 2001 г. в структуре МВД России создано специализированное подразделение – Управление «К» БСТМ МВД России, у которого основными направлениями оперативно-служебной деятельности являются:

- 1) борьба с преступлениями в сфере компьютерной информации;
- 2) борьба с преступлениями в сфере телекоммуникаций;
- 3) борьба с незаконным оборотом РЭС и СТС;
- 4) борьба с нарушением авторских и смежных прав;
- 5) борьба с распространением детской порнографии;
- 6) борьба с преступлениями в электронных платежных системах.

Для достижения цели, системного анализа и принятия решений, исходя из складывающихся оперативно-следственных ситуаций в ходе раскрытия преступлений, совершаемых в информационно телекоммуникационных системах, было и предложено данное исследование.

Компьютеризация всех слоев населения носит социально значимое влияние, но его достижения могут быть использованы не только в благих целях, но и при совершении преступлений компьютерной направленности. *Компьютерные преступления* носят специфичный характер и в настоящее время – это новации в системе уголовного права, так как способы их совер-

шения настолько многогранны и носят изощренный характер, что порой сотрудникам управлений «К» при документировании и раскрытии данного вида преступлений приходится сталкиваться с определенными трудностями, в связи с чем разрабатываются и внедряются новые формы и методы оперативно-розыскной деятельности. Необходимо заметить, что одним из важнейших составляющих элементов криминалистической характеристики в ходе раскрытия компьютерных преступлений является *субъективная особенность личности* преступника, который на начальном этапе раскрытия преступлений характеризуется лишь скудной информацией. В связи с этим мы абсолютно согласны с мнением, высказанным Т.В. Ворошиловой, которая предлагает учитывать такие составляющие, как пол, возраст, социальное происхождение, уровень образования, род занятий, наличие специальности, семейное положение, социальный статус, уровень материальной обеспеченности, место жительства, а также места проведения досуга и возможная принадлежность к определенной субкультуре [2]. Иными словами, немаловажное значение в раскрытии любого вида компьютерного преступления играет *характерологическая особенность психологии личности преступника*, которая позволяет при глубоком анализе определить и сузить круг подозреваемых лиц, мотив преступления, способ его совершения, а также выдвинуть версии, что естественно приблизит оперативных работников и следователей к осуществлению выполнения оперативно-розыскных мероприятий и следственных действий, способствующих раскрытию данного вида преступлений. Между тем отечественное уголовное законодательство обеспечивает правовую защиту наряду с документированной информацией и иным её разновидностям и, следовательно, расширяет представление о предмете криминальной деятельности. Анализ действующего Уголовного кодекса РФ показывает, что законодатель выделил из всего объема информационных отношений как подлежащие специальной охране отношения, возникающие в области компьютерной информации. В главу 28 УК РФ о преступлениях в сфере компьютерной информации введены термины и понятия, которых ранее не было не только в уголовно-правовой терминологии, но и в законодательстве, регулировавшем информационные отношения.

Проанализировав нормы из различных отраслей права, можно сделать ряд *выводов*:

1. Информацией является совокупность предназначенных для передачи формализованных знаний и сведений о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [3].

2. Правовой защите подлежит любая документированная информация, то есть информация, облеченная в форму, позволяющую ее идентифицировать [4].

3. Документированная информация является объектом гражданских прав и имеет собственника.

4. Информация может быть *конфиденциальной*, ознакомление с которой ограничивается ее собственником или нормами закона, и *массовой*, предназначенной для неограниченного круга лиц [5].

5. Ограничения (установление режима) использования информации устанавливаются законом или собственником информации, которые объявляют уровень ее конфиденциальности.

Конфиденциальными в соответствии с законом являются, в частности, такие *виды информации*, как:

- содержащая государственную тайну [6];
- передаваемая путем переписки, телефонных переговоров, почтовых телеграфных или иных сообщений [7];

- содержащая служебную тайну [8], коммерческую тайну [9], банковскую тайну [10], личную тайну и семейную тайну [11], информация, являющаяся объектом авторских и смежных прав [12];

- непосредственно затрагивающая права и свободы гражданина или персональные данные [13] и др.

6. Любая форма завладения и пользования конфиденциальной документированной информацией без прямо выраженного согласия ее собственника является нарушением его прав, то есть *неправомерной*;

Уголовно-правовой анализ преступлений в сфере компьютерной информации невозможно провести без предварительного уяснения родового понятия информации. Она выступает в качестве сравнительно нового предмета исследования и особого объекта правового регулирования. Именно поэтому необходимо обратиться не только к законодательным понятиям информации, но и к *научным ее толкованиям*.

Понятие «информация» имеет как минимум четыре основных значения:

- как сведения, передаваемые людьми любым способом;
- как общенаучное понятие;
- как обмен сигналами в животном и растительном мире;
- как кибернетический термин.

Само слово «информация» происходит от латинского «information» и означает «разъяснение» или «осведомленность» [14]. Начальные шаги в теории информации были сделаны еще в первой половине XX в.: в 1928 г. Р. Хартли впервые дал количественное определение информации, а в 1948 г. вышла знаменитая книга К. Шеннона «Математическая теория связи», где информация и дается уже как статистическое определение.

Н. Винер, один из основателей кибернетики, определил информацию как «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств» [15]. К. Шеннон, который сыграл не меньшую роль в развитии кибернетики, рассматривал информацию как сигнал (сообщение), устраняющий или снижающий неопределенность [16].

А.А. Фатьянов полагает, что «информация есть воспринимаемая живым организмом через органы чувств окружающая действительность в виде распределения материи и энергии во времени и в пространстве и процессов их перераспределения».

Таким образом, информация с точки зрения кибернетики представляется не как общественный феномен, то есть информация, производимая и потребляемая обществом, а в более узком, техническом аспекте – как информация, циркулирующая по электронным каналам связи. Кибернетика доказала, что информация имеет непосредственное отношение к процессам управления и развития, обеспечивающим функционирование любых систем.

Информационная сфера сегодня – это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающаяся в адекватном правовом регулировании. С этой целью создается «информационное» законодательство, а также система мер уголовно-правовой защиты данной группы отношений. Последние изменения в главу 28 УК РФ вступили в силу 7 декабря 2011 г.

Основное различие правового режима информации состоит в степени ее доступности для пользователей. Так, в зависимости от категории доступа к ней информация подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) [17]. В соответствии со ст. 5 Федерального закона ФЗ-№ 149 от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации», информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- 1) информацию, свободно распространяемую;
- 2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- 3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- 4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Так, например, правовой режим информации, составляющей государственную тайну, определяется Законом РФ № 5485-1 от 21.07.1993 г. «О государственной тайне» (с изменениями от 06.10.1997 г.) [18]. Перечень сведений, составляющих государственную тайну, определен ст. 5 Закона и включает в себя три основных раздела:

- 1) сведения в военной области;
- 2) сведения в области экономики, науки и техники;
- 3) сведения в области внешней политики и экономики.

Как указывалось ранее, законодателю в каждом нормативно-правовом акте требуется найти баланс между обеспеченным Конституцией РФ правом граждан на информацию и обеспечением ее конфиденциальности. Не стал исключением в этом смысле и Закон «О государственной тайне», который содержит перечень сведений, не подлежащих отнесению к государственной тайне и засекречиванию.

В соответствии со ст. 7 Закона таковыми являются: сведения о чрезвычайных происшествиях, катастрофах, стихийных бедствиях; о состоянии экологии, здравоохранения, санитарии, демографии, а также о состоянии преступности; о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам; о фактах нарушения прав и свобод человека и гражданина; о размерах золотого запаса и государственных валютных резервах РФ; о состоянии здоровья высших должностных лиц РФ; о фактах нарушения законности органами государственной власти и их должностными лицами.

Основополагающие принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации заложены ФЗ «Об информации, информационных технологиях и о защите информации», в ст. 3 которого четко установлено, что правовое регулирование рассматриваемых отношений основывается на принципах:

- 1) свободы поиска, получения, передачи, производства и распространения информации любым законным способом;

- 2) установления ограничений доступа к информации только федеральными законами;
- 3) открытости информации о деятельности государственных органов и органов местного самоуправления и свободного доступа к такой информации, кроме случаев, установленных федеральными законами;
- 4) равноправия языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- 5) обеспечения безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- 6) достоверности информации и своевременности ее предоставления;
- 7) неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- 8) недопустимости установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Понятие «*компьютерной информации*» является не менее многозначным, чем понятие информации. Ее место в системе правоотношений, возникающих в информационной сфере, до сих пор является предметом научных дискуссий, которые пока не завершились формированием общепризнанного научного и законодательного определения, поскольку многообразие его толкования отображает весьма сложный характер реального мира.

Проблемы в правоприменительной практике связаны с тем, что, несмотря на важность точного формализованного представления о сущности и свойствах компьютерной информации (как предмета преступления), *на законодательном уровне определение «компьютерной информации» появилось относительно недавно*. Однако в специальной и учебной литературе предложено множество определений рассматриваемого термина. Так, например, одними из первых понятие «компьютерной информации» дали: Т.Г. Смирнова, определив компьютерную информацию как «совокупность сведений, представляющих особую ценность для государства, общества и отдельных граждан, производство, хранение и использование которых осуществляется посредством компьютерной техники», и А. Петров, предложивший понимать под данным термином «информацию, содержащую сведения, составляющие государственную или коммерческую тайну, сведения конфиденциального характера и общего пользования».

Отметим, что предложенные определения не лишены недостатков. Из определения Т.Г. Смирновой следует, что информация и ее материальный носитель («компьютерная техника») не отделимы друг от друга, а исходя из такого подхода, компьютерная информация, циркулирующая в сети ЭВМ, не будет являться предметом данной категории преступлений, а, следовательно, останется без надлежащей уголовно-правовой защиты. Из содержания понятия «компьютерная информация», данного А.А. Петровым, вообще невозможно выделить отличительные признаки компьютерной информации как таковой [19].

Более корректными представляются определения, предложенные С.А. Пашиным и В.С. Комиссаровым. По утверждению первого автора, «компьютерная информация – это информация, зафиксированная на *машинном носителе или передаваемая по телекоммуникационным каналам* в форме, доступной восприятию ЭВМ» [20]. В.С. Комиссаров справедливо указал, что «компьютерная информация может находиться или на машинном носителе (магнитном диске, магнитной ленте, дискете, магнитно-оптическом диске (CD-ROM), или непосредственно в ЭВМ (в постоянном или оперативном запоминающих устройствах), либо в системе ЭВМ или их сети» [21]. По нашему мнению предложенные С.А. Пашиным и В.С. Комиссаровым понятия наиболее точные, четко отражают критерии предмета преступлений в сфере компьютерной информации. Также нельзя не согласиться и с определением «компьютерного преступления», предложенным авторами В.А. Дуленко, Р.Р. Мамлеевым, В.А. Пестриковым, где ими сказано, что компьютерное преступление как уголовно-правовое понятие – это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства [22].

Поэтому с учетом представленных позиций авторов по нашему видению понятие «компьютерной информации» как предмета преступления можно сформулировать **как организационно упорядоченную совокупность сведений (сообщений, данных), зафиксированных на машинном носителе либо в информационно-телекоммуникационной сети с реквизитами, позволяющими их идентифицировать, имеющую собственника либо иного законного владельца**.

Полагаем, что уголовно-правовой защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее собственнику (владельцу, пользователю). При закреплении предложенного определения в базовом для этой сферы законодательстве, напри-

мер в Федеральном законе «Об информации, информационных технологиях и о защите информации», оно позволит, на наш взгляд, существенно сократить ошибки в правоприменении рассматриваемых уголовно-правовых норм.

Как уже было сказано выше, одним из *современных* видов компьютерных преступлений являются преступления в *сфере телекоммуникаций*.

В настоящее время, по нашему мнению, *телекоммуникационные системы внедряются во все сферы жизнедеятельности человека и представляют собой сеть развитых технических средств по сбору, передаче, обработке и хранению информации*, и они наиболее часто подвержены пристальному вниманию со стороны преступников.

В соответствии со ст. 2 Федерального закона «Об информации, информатизации и защите информации» и ч. 1 ст. 272 УК РФ, *«информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления»* [23]. Хочется привести еще одно определение компьютерной информации, которое дается доцентом кафедры криминалистики МГУ им. М.В. Ломоносова В. Крыловым, предлагающим следующее криминалистическое определение компьютерной информации как *специального объекта преступного посягательства*: компьютерная информация есть сведения, знания или набор команд (программа), предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях – идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования.

Таким образом, *правовой защите* подлежит главным образом *документированная информация* (документ), зафиксированная на материальном носителе с реквизитами, то есть информация, которая облечена в форму, позволяющую ее «идентифицировать» [24].

Кроме того, понятие *«документированная информация»* основано на «двуединстве – информации (сведений) и материального носителя, на котором она отражена в виде символов, знаков, букв, волн или других способов отображения. В результате документирования происходит как бы материализация и овеществление сведений...» [25]. Отсюда можно сделать вывод, что информация становится объектом гражданского законодательства.

Любое преступление, совершаемое в сфере телекоммуникаций, как уже ранее было сказано, является одним из разновидностей преступлений в сфере компьютерной информации. Все они обладают следующими *криминалистическими особенностями*:

1. Эта информация достаточно просто и быстро *преобразуется* из одной объектной формы в другую, копируется (размножается) на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств телекоммуникационных сетей.

2. При изъятии (копировании) информации, зафиксированной в телекоммуникационных сетях, а также любого вида компьютерной информации, в отличие от изъятия *материального предмета*, она может *сохраниться* в первоисточнике.

3. Любая информация, в том числе и телекоммуникационная, становится *продуктом* общественных отношений, имеет определенную *цену* и является *предметом* купли-продажи.

Такого рода общественные отношения закреплены в Федеральном законе «Об информации, информатизации и защите информации». В связи с этим новые информационные технологии не только дали толчок в плане прогресса общества, но и стимулировали возникновение и развитие новых форм преступности. Прогресс в области компьютерной техники и *телекоммуникационной среде* предоставил злоумышленникам широкие возможности неправомерного доступа к новым техническим средствам и дальнейшее их использование в противоправных целях.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. См.: *Винер Н.* Кибернетика и общество. – М., 2003. – С. 31.
2. *Ворошилова Т.В.* Социальная и психологическая характеристика личности компьютерного преступника. – М., 2009. – С. 5.
3. Об информации, информатизации и защите информации: Федеральный закон.
4. Там же. Ст. 2.
5. Там же.
6. 6.О государственной тайне: ФЗ РФ от 21 июля 1993 г. № 5485-1; УК РФ, ст. 275, 276, 283, 284.
7. Конституции РФ, ст.23, ч.2; УК РФ, ст.138.
8. ГК РФ, ст.139.
9. ГК РФ, ст. 139; УК РФ, ст. 183.
10. УК РФ, ст.183.
11. УК РФ, ст.137.
12. Об авторском праве и смежных правах: Закон РФ; УК РФ, ст.146.
13. Об информации, информатизации и защите информации: Федеральный закон; УК РФ, ст.140.
14. Большой энциклопедический словарь. – М., 2004. – С. 421.

15. *Винер Н.* Кибернетика и общество. – М., 2003. – С. 35.
16. *Шеннон К.* Работы по теории информации и кибернетики. – М., 1963. – С. 59.
17. *Фатьянов А.А.* Правовое обеспечение безопасности информации в Российской Федерации: Учеб. пособие. – М., 2001. – С. 10.
18. СЗ РФ 1997г., № 41. Ст. 4673.
19. См.: *Петров А.А.* Компьютерная информация как предмет уголовно-правовой защиты реформированного уголовного законодательства // Российское право в период социальных реформ. – Н.Новгород. 1998. Вып. 2. – С. 132.
20. Комментарий к Уголовному кодексу Российской Федерации / Под общ. ред. Ю.И. Скуратова, В.М. Лебедева. – М., 2001. – С. 696.
21. Уголовное право России / Под ред. В.С. Комисарова. – М., 2006. – С. 307.
22. *Дуленко В.А., Мамлеев Р.Р., Пестриков В.А.* Преступление в сфере высоких технологий: Учебное пособие. – М, 2010. – С. 196.
23. Об информации, информатизации и защите информации: Федеральный закон от 20 февр. 1995 г. № 24-ФЗ. Ст.2.
24. *Крылов В.В.* Информация как элемент криминальной деятельности // Вестник Московского университета. Сер. 11. – М.: Право, 1998. – №4.
25. *Копылов В.А.* Информационное право. – М.: Юристъ, 1997. – С. 23.

REFERENCES

1. Sm.: *Viner N.* Kibernetika i obshchestvo. - M., 2003. - S. 31.
2. *Voroshilova T.V.* Sotsialnaya i psikhologicheskaya kharakteristika lichnosti kompyuternogo prestupnika. - M., 2009. - S. 5.
3. Ob informatsii, informatizatsii i zashchite informatsii: Federalnyy zakon.
4. Tam zhe. St. 2.
5. Tam zhe.
6. O gosudarstvennoy tayne: FZ RF ot 21 iyulya 1993 g. № 5485-1; UK RF, st. 275, 276, 283, 284.
7. Konstitutsii RF, st.23, ch.2; UK RF, st.138.
8. GK RF, st.139.
9. GK RF, st. 139; UK RF, st. 183.
10. UK RF, st.183.
11. UK RF, st.137.
12. Ob avtorskom prave i smezhnykh pravakh: Zakon RF; UK RF, st.146.
13. Ob informatsii, informatizatsii i zashchite informatsii: Federalnyy zakon; UK RF, st.140.
14. Bolshoy entsiklopedicheskiy slovar. - M., 2004. - S. 421.
15. *Viner N.* Kibernetika i obshchestvo. - M., 2003. - S. 35.
16. *SHennon K.* Raboty po teorii informatsii i kibernetiki. - M., 1963. - S. 59.
17. *Fatyanov A.A.* Pravovoe obespechenie bezopasnosti informatsii v Rossiyskoy Federatsii: Ucheb. posobie. - M., 2001. - S. 10.
18. SZ RF 1997g., № 41. St. 4673.
19. Sm.: *Petrov A.A.* Kompyuternaya informatsiya kak predmet ugovovno-pravovoy zashchity reformirovannogo ugovovnogo zakonodatelstva // Rossiyskoe pravo v period sotsialnykh reform. - N.Novgorod. 1998. Vyp. 2. - S. 132.
20. Kommentariy k Ugolovnomu kodeksu Rossiyskoy Federatsii / Pod obshch. red. YU.I. Skuratova, V.M. Lebedeva. - M., 2001. - S. 696.
21. Ugolovnoe pravo Rossii / Pod red. V.S. Komisarova. - M., 2006. - S. 307.
22. *Dulenko V.A., Mamleev R.R., Pestrikov V.A.* Prestuplenie v sfere vysokikh tekhnologiy: Uchebnoe posobie. - M, 2010. - S. 196.
23. Ob informatsii, informatizatsii i zashchite informatsii: Federalnyy zakon ot 20 fevr. 1995 g. № 24-FZ. St.2.
24. *Krylov V.V.* Informatsiya kak element kriminalnoy deyatel'nosti // Vestnik Moskovskogo universiteta. Ser. 11. - M.: Pravo, 1998. - №4.
25. *Kopylov V.A.* Informatsionnoe pravo. - M.: YUrist, 1997. - S. 23.