Дмитрий Михайлович МОЛЧАНОВ,
доцент кафедры уголовного права Университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук, доцент
dmmolchanov@msal.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Информационная безопасность как объект охраны от агрессивного информационного воздействия

Аннотация. *В статье предлагается рассматривать информационную безопасность как трехсоставной объект, который включает в себя защищенность полезной информации от внешнего воздействия; доступность достоверной информации для обеспечения нормального функционирования государственных институтов и жизнедеятельности граждан; защищенность человека от агрессивного или деструктивного информационного воздействия. Основное внимание уделяется последнему аспекту. Существуют два механизма защиты: личный информационный фильтр, основанный на верном понимании ценностной иерархии, и принудительное ограничение информационных потоков со стороны государства. Ни тот ни другой механизм в настоящее время полноценно не работает: субъективная ценностная иерархия большого числа людей не соответствует объективной картине мира, а государство пока не научилось ни контролировать, ни ограничивать информационные потоки. Информационная среда в России очень неоднородна, огромное количество деструктивной информации находится в открытом доступе. Возможность генерирования и распространения такой информации почти не ограничена. Но осознание проблемы уже появилось и попытки выстраивания информационных барьеров как в направлении воспитания верных нравственных ориентиров, так и в направлении контроля и регулирования информационных потоков в России предпринимаются.*

Ключевые слова: *информационная безопасность, агрессивная информационная среда, ценностная иерархия, информационное воздействие, информационные фильтры, традиционные духовно-нравственные ценности, защищенность от информации, адресное информационное воздействие, публичное информационное воздействие, информационная атака*

DOI: 10.17803/2311-5998.2025.129.5.074-083

Dmitry M. MOLCHANOV,
Associate Professor of the Department of Criminal Law
of the Kutafin Moscow State Law University (MSAL),
Cand. Sci. (Law), Associate Professor
dmmolchanov@msal.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Information Security as an Object of Protection from Aggressive Information Influence

Abstract. *The article proposes to consider information security as a three-component object, which includes the protection of useful information from external influence, the availability of reliable information to ensure the normal functioning of state institutions and the life of citizens, and the protection of a person from aggressive or destructive information impact. The main attention is paid to the last aspect. There are two mechanisms of protection: a personal information filter based on the correct understanding of the value hierarchy and forced restriction of information flows by the state. Neither mechanism is currently fully operational: the subjective value hierarchy of a large number of people does not correspond to the objective picture of the world, and the state has not yet learned to either control or limit information flows. The information environment in Russia is very heterogeneous, a huge amount of destructive information is in the public domain. The possibility of generating and disseminating such information is almost unlimited. But awareness of the problem has already appeared and attempts to build information barriers both in the direction of educating the correct moral guidelines and in the direction of control and regulation of information flows in Russia are being undertaken.*
Keywords: *information security, aggressive information environment, value hierarchy, information impact, information filters, traditional spiritual and moral values, protection from information, targeted information impact, public information impact, information attac*

В начале было Слово, и Слово было у Бога,
и Слово было Бог.
Ин. 1:1
И сказал Бог: да будет свет. И стал свет.
Быт. 1:3

Стоящие эпиграфом к данному исследованию слова из Евангелия от Иоанна и Книги Бытия имеют онтологический смысл и не требуют подробного анализа в этой работе, поскольку мы изучаем проблематику более низкого уровня, однако они могут являться камертоном, позволяющим настроиться на понимание масштаба исследуемых проблем: разрушительная сила слова может быть колоссальна. Словом созданный стройный порядок мироздания разрушается человеческими словами и возвращается к первобытному доисторическому состоянию хаоса: таков масштаб. Та информация, то слово, которое является

предметом изучения, образно и метко описано Н. С. Гумилевым в последнем четверостишии его одноименного стихотворения:

Мы ему поставили пределом
Скудные пределы естества.
И, как пчелы в улье опустелом,
Дурно пахнут мертвые слова.

О мертвых словах, об информации, разрушающей сознание, а вслед за этим и все окружающее, и пойдет речь в данной статье.

Безопасность в уголовном праве традиционно понимается как состояние защищенности. Применительно к информационной безопасности можно выделить минимум три аспекта: защищенность информации, защищенность от информации и защищенность права обладания достоверной информацией, имеющей жизненно важное (в широком смысле) значение для конкретного человека или нормальной деятельности государственных органов Российской Федерации. В первом случае речь идет об обеспечении безопасности ценной информации от деструктивного внешнего воздействия, во втором — о защите от деструктивного внешнего воздействия самой информации[1] на человека, в третьем — о защите права на обладание жизненно необходимой достоверной информацией, которая утаивается.

Необходимость охраны информации для законодателя очевидна, поэтому в УК РФ в зависимости от специфики охраняемой информации нормы о ее защите обособляются самим законодателем либо в отдельную группу в одной главе (например, преступления в сфере компьютерной информации), либо в группу, хотя и не обособленную, но помещенную в одну главу наряду с иными преступлениями (например, преступления, посягающие на сохранность государственной тайны). Защита права на обладание достоверной информацией обеспечивается несколькими нормами УК РФ, в которых устанавливается ответственность за непредоставление информации или за предоставление недостоверной информации.

Однако право на обладание достоверной информацией не рассматривается ни законодателем, ни доктриной уголовного права в качестве составной части более общего объекта охраны: информационной безопасности. Да и само право на обладание достоверной информацией в большинстве случаев является дополнительным объектом, однако и эта характеристика состава зачастую в доктрине игнорируется[2]. Исключение составляют ст. 140 и 287 УК РФ.

---

[1] В теории дается различное толкование термина «информация». См., например: *Кузьмин В. П.* Понятие и юридическая сущность информации // Информационное право. 2009. № 2. С. 6.

[2] Например, в Комментарии к УК РФ под редакцией В. М. Лебедева для ст. 237 УК РФ право граждан на получение достоверной информации указывается как дополнительный объект, а в других комментариях наличие дополнительного объекта игнорируется (см., например: Комментарий к Уголовному кодексу Российской Федерации : в 4 т. М. : Юрайт, 2017. Т. 3 : Особенная часть / отв. ред. В. М. Лебедев. С. 122 ; Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. И. Чучаева. 3-е изд., испр. и доп. М. : Контракт, 2011. С. 349.

Конституционно закрепленное право (ст. 24 Конституции РФ) на обладание достоверной информацией, содержащейся в документах и материалах, непосредственно затрагивающих права и свободы человека, является основным непосредственным объектом нормы, закрепленной в ст. 140 УК РФ. Непосредственным объектом нормы, закрепленной в ст. 287 УК РФ, являются общественные отношения в области полноценного информационного обеспечения Федерального Собрания РФ и Счетной палаты РФ. Криминализация деяний, закрепленных в остальных нормах УК РФ, устанавливающих запрет на непредоставление информации или предоставление недостоверной информации, обусловливается необходимостью охраны иных объектов: интересов инвесторов (ст. 185[1]), интересов кредиторов (ст. 195), общественной безопасности в широком смысле (ст. 207[1]), общественной безопасности в части охраны жизни и здоровья граждан (ст. 207[2]), здоровья населения (ст. 237).

В отношении непосредственного объекта уголовно-правовой охраны нормы, закрепленной в ст. 237 УК РФ, следует отметить, что он выходит за пределы видового объекта гл. 25 УК РФ, поскольку название статьи определяет, что сокрытие информации создает опасность не только для здоровья, но и для жизни людей (видовой объект гл. 24 УК РФ), а диспозиция статьи позволяет говорить и о том, что непосредственный объект вторгается в пределы видового объекта гл. 26 УК РФ, поскольку указывает на угрозу наступления негативных последствий для окружающей среды.

Следовательно, можно утверждать, что это своего рода межвидовая норма, которая соответствует объему родового объекта, но выходит за пределы трех видовых объектов глав 24, 25 и 26 УК РФ. Кратко сто́ит упомянуть и о том, что место информационной безопасности как объекта уголовно-правовой охраны этой нормы не всегда верно понимается в теории. Так, в комментарии к УК РФ под редакцией профессора А. В. Бриллиантова можно встретить утверждение, что основным непосредственным объектом являются «общественные отношения, обеспечивающие право гражданина на получение достоверной информации об обстоятельствах, создающих опасность для жизни или здоровья», а факультативным объектом — «отношения по охране здоровья, окружающей природной среды»[3].

Согласиться с этой позицией нельзя, поскольку общественная безопасность в части защищенности жизни людей, здоровья населения и безопасной окружающей среды является не факультативным, а основным непосредственным объектом данной нормы. Именно создание угрозы этому объекту обусловливает возможность наступления уголовной ответственности. А в механизм возможного причинения вреда основному объекту включается объект дополнительный: информационная безопасность в части осведомленности населения о фактах и обстоятельствах, угрожающих экологии, жизни и здоровью людей. В ряде доктринальных источников мы находим именно такое понимание непосредственного и дополнительного объектов[4].

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. В. Бриллиантова : в 2 т. 2-е изд. М. : Проспект, 2015. Т. 2. С. 130.

[4] См., например: Комментарий к Уголовному кодексу Российской Федерации : в 4 т. Т. 3. С. 122.

Значимость достоверной информации для обеспечения безопасности населения существенно возрастает при появлении дополнительных угроз. Например, военные действия, которые Российская Федерация вынужденно вела на своей территории в Курской области, являются ответом на возникшую угрозу территориальной целостности и жизни населения России. А предоставление несвоевременной и недостоверной информации о возникшей угрозе в самом начале ее появления, в том числе в средствах массовой информации, создало препятствие в принятии мер по своевременной эвакуации населения, что повлекло тяжкие последствия для оставшегося на оккупированной территории населения, в отношении которого представителями вооруженных сил противника совершались различные преступления: убийства, причинение различной тяжести вреда здоровью, изнасилования, грабежи, разбои.

Изучение судебной практики (если такая имеется), в связи с вышеизложенными обстоятельствами, о привлечении каких-либо лиц к уголовной ответственности по статьям 207^1 или 207^2 УК РФ могло бы быть основой отдельного научного исследования. Если такой практики нет, то это хороший повод для исследования другой проблемы: пробелов в УК РФ в части установления уголовной ответственности за несвоевременное и недостоверное информирование населения об угрозах, возникающих вследствие военных действий.

Столь длинный экскурс по объекту исследования потребовался нам по той причине, что в доктрине уголовного права России пока еще не устоялось понимание информационной безопасности как трехсоставного объекта[5].

Обратимся к теоретическим и практическим аспектам информационной безопасности как объекта охраны от деструктивного информационного воздействия. Какие угрозы информационной безопасности в этой сфере существуют? Есть ли эффективные уголовно-правовые механизмы борьбы с этими угрозами? Что собой представляет информационная безопасность как объект охраны в этой сфере?

Как выглядит проблема глазами законодателя? Во-первых, в Особенной части УК РФ есть ряд норм, прямо запрещающих распространение деструктивной информации[6]; во-вторых, законодатель усиливает ответственность за ряд

---

[5] В доктрине уголовного права представлены в основном многочисленные попытки осмысления отдельных частей этого объекта. См., например: *Чеботарева А. А.* Обеспечение информационной безопасности личности в Интернете: история и проблемы развития законодательства // История государства и права. 2010. № 11. С. 30—33 ; *Ефремова М. А.* Информационная безопасность как объект уголовно-правовой охраны // Информационное право. 2014. № 5. С. 21—25.

[6] Например, эти нормы закреплены в следующих статьях УК РФ: ст. 110^2 «Организация деятельности, направленной на побуждение к совершению самоубийства»; ст. 205^2 «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма»; ст. 280 «Публичные призывы к осуществлению экстремистской деятельности»; ст. 280^1 «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации»; ст. 280^4 «Публичные призывы к осуществлению деятельности, направленной против безопасности государства»; ст. 282^4 «Неоднократные пропаганда

преступлений, которые сами по себе не несут угрозы информационной безопасности, однако в сочетании с инструментами по распространению информации создают качественно новую угрозу, поскольку демонстративно выставляются напоказ неограниченно широкой аудитории сети Интернет. Большое число статей УК РФ, предусматривающих ответственность за насильственные преступления (например, п. «о» ч. 2 ст. 105, п. «и» ч. 2 ст. 111, п. «д» ч. 2 ст. 115, п. «и» ч. 2 ст. 126, п. «з» ч. 2 ст. 127 УК РФ), дополнено квалифицирующим признаком следующего содержания: «совершенное с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)».

В-третьих, в ряде норм, которые относятся к квалифицированным составам, в качестве квалифицирующего признака указывается на совершение этого преступления с использованием такого информационного инструмента, как сеть Интернет (например, в п. «б» ч. 3 ст. 133 ; п. «в» ч. 3 ст. 222 ; п. «б» ч. 2 ст. 228[1] УК РФ). Информационную безопасность в таких случаях вполне уместно считать дополнительным объектом, поскольку именно легкий доступ к информации создает предпосылки для огромного спектра негативных последствий, которые появляются у лица, подвергшегося информационному воздействию. Возможность обезличенного общения через Интернет создает «рабочие места» для посредников в сбыте или приобретении оружия или наркотиков, создает комфортные условия для приобретения запрещенных предметов без опасения быть привлеченным к уголовной ответственности.

И главной точкой приложения усилий со стороны государства для борьбы с этими преступлениями могло бы быть пресечение беспрепятственного обмена информацией в этой сфере. Следует отметить и явную недооценку степени общественной опасности преступлений, совершаемых с использованием сети Интернет: на основе опыта так называемых цветных революций можно было бы сделать однозначный вывод о том, что данный квалифицирующий признак необходим в ст. 212 УК РФ, предусматривающей ответственность за организацию массовых беспорядков, но такого признака нет.

На основе анализа судебной практики можно сделать вывод о том, что огромное число преступлений, предусмотренных ст. 135 УК РФ, совершается с использованием сети Интернет, но такого признака и здесь нет. Исходя из многофункциональности сети Интернет как средства передачи информации, можно было бы учитывать его использование как обстоятельство, отягчающее наказание, но ст. 63 УК ограничивается усилением ответственности лишь за один вариант его использования: для публичной демонстрации совершаемого преступления. Объяснить это можно тем, что пока государство находится в самом начале пути осознания глобальности угроз для всех сфер жизнедеятельности государства, создаваемых возможностью неконтролируемого информационного воздействия.

либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами»; ст. 354 «Публичные призывы к развязыванию агрессивной войны».

Потенциально нормы УК РФ, запрещающие противоправное информационное воздействие, наряду с теми объектами, которые закладываются в них законодателем и легко считываются при обычном подходе к толкованию исходя из места нормы в структуре Особенной части УК, охраняют и информационную безопасность. Например, норма, устанавливающая уголовно-правовой запрет на клевету (ст. 128[1] УК РФ), вряд ли воспринимается как норма, защищающая информационную безопасность. Традиционно принято считать, что клевета посягает на такие объекты уголовно-правовой охраны, как честь и достоинство. Это, конечно же, верно, однако ни законодатель, ни правоприменитель, ни доктрина уголовного права не учитывают тот факт, что ложная информация, порочащая честь и достоинство другого человека, не менее разрушительно действует и на людей, которые воспринимают такую информацию, поскольку они становятся носителями негативного отношения к другим людям, осуждают их, испытывают негативные эмоции, может быть, даже проявляют готовность порвать или рвут социальные связи в самых различных сферах (семейные, творческие, деловые и пр.), хотя никаких оснований для этого нет, поскольку информация, которой они поверили, не соответствует действительности. Вряд ли законодатель учитывал эти угрозы. Но они существуют, и дальнейшая теоретическая разработка этой темы позволит и законодателю учитывать все грани общественной опасности деструктивной информации.

Необходимо отметить, что деструктивное информационное воздействие может быть адресным, а может носить публичный характер. К адресному воздействию на ограниченный круг субъектов можно отнести те случаи, когда одно лицо побуждает другое лицо к совершению какого-либо преступления. Такие действия могут получить оценку как соучастие в виде подстрекательства, а могут рассматриваться законодателем в качестве самостоятельного преступления в статьях Особенной части[7].

Адресное воздействие, побуждающее совершить то или иное негативное действие, может быть самостоятельным преступлением, не являясь аналогом соучастия (ст. 150, 151 УК РФ). На примере ст. 150 УК РФ можно уяснить интересную закономерность: по смыслу данной статьи вовлекаемый в совершение преступления несовершеннолетний является потерпевшим, что не исключает возможности привлечения его самого к уголовной ответственности в качестве соучастника того преступления, в которое его вовлекли. Взрослый человек, которого подстрекатель вовлек в совершение преступления, сделав своим соучастником, в юридическом смысле, конечно же, не может признаваться потерпевшим, но, рассматривая действия подстрекателя в контексте нарушения информационной безопасности, вполне можно утверждать, что подстрекаемый — именно жертва деструктивного информационного воздействия. Потерпевшие же в буквальном смысле слова могут подвергаться агрессивному информационному воздействию различной направленности. Например, мошенничество, развратные действия, склонение к потреблению наркотических средств — это те преступления, которые невозможно совершить без оказания деструктивного информационного воздействия на потерпевшего.

---

[7] См., например: УК РФ. Ч. 1 и 1[1] ст. 205[1].

Массовое информационное воздействие может быть следующих видов: 1) массовое воздействие, побуждающее к противоправным действиям (в том числе к преступлениям); 2) массовое воздействие, направленное на нравственное разрушение человеческой личности или причинение иного вреда, причем направленность в данном случае может являться объективной характеристикой, которая может и не осознаваться самим преступником. Возможно сочетание адресного и массового воздействия, когда информационная атака, хотя и носит адресный характер (например, при мошенничестве), однако совершается на постоянной основе в отношении большого количества потерпевших (например, массовый обзвон).

Опасность деструктивного информационного воздействия обусловлена тем, что в человеческой природе заложена склонность к информационному взаимодействию друг с другом и естественной реакцией является доверие. Это особенно ярко проявляется в детях, которые без сомнения воспринимают все, что слышат от родителей. С возрастом у человека появляется навык критического мышления, и всякая новая информация воспринимается избирательно, в зависимости от той схемы информационных фильтров, которая в человеке сформирована. Главная проблема заключается в том, что схема фильтрации изначально у большинства людей сформирована с изъянами и может работать в обратном направлении: нужную и жизненно важную для человека информацию отвергать, а разрушительную и негативную воспринимать как полезную.

Этим словам более 2 700 лет, но с тех пор люди не изменились[8]: «Горе тем, которые зло называют добром, и добро — злом, тьму почитают светом, и свет — тьмою, горькое почитают сладким, и сладкое — горьким! Горе тем, которые мудры в своих глазах и разумны пред самими собою!» (Ис. 5:20—21). Полная неадекватность в восприятии информации встречается, наверное, редко, а возможно, вообще не встречается, если только речь не идет о психических патологиях. А вот частичное смещение ориентиров в большей или меньшей степени — явление повсеместное. Это обусловливается в первую очередь тем, что ценностная иерархия большинства людей не имеет объективной основы: добро и зло воспринимаются как понятия относительные.

Это означает, что большинство людей представляют группу повышенного риска: неспособность отделить зерна от плевел позволяет деструктивной информации завладевать сознанием человека и в первую очередь разрушать его изнутри, а затем побуждать его нести разрушительную энергию во внешний мир в виде самых разнообразных преступлений. В какую именно брешь проникнет информация, зависит от индивидуальной деформации: кого-то можно убедить в национальной исключительности, кого-то в бессмысленности жизни и необходимости покончить жизнь самоубийством, кого-то — в том, что необходимо бороться за права сексуальных меньшинств. В случае, если внутренние информационные

[8] Люди не изменились, но очень сильно изменились внешние условия, изменилось информационное поле. Если раньше человек жил в пустыне своего разума и ему попадались лишь информационные ручейки с возможностью выбора, из какого попить, то сегодня он живет в море информации, в которое впадают тысячи рек, бóльшая часть которых — сточные канавы.

фильтры работают с правильной настройкой (на основе объективно верной системы ценностей), вероятность воздействия деструктивной информации остается, но является низкой.

Углубляться в детальное рассмотрение субъективной картины мира конкретного человека, максимально приближенной к объективной ценностной реальности, в рамках данной статьи мы не можем, но можем проиллюстрировать, как работает механизм защиты в этом случае, на частном примере. Например, ст. 282[4] УК РФ запрещает пропаганду либо публичное демонстрирование нацистской атрибутики или символики, поскольку существует риск закрепления в сознании людей таких знаков и символов как положительных, с дальнейшим перенесением этих характеристик символов на их носителей как людей «сильных, твердых, решительных», однако для выживших узников концлагерей такая символика не может вызывать ничего, кроме отвращения, поскольку они имели опыт реального общения с этими «сильными, твердыми и решительными» людьми, носившими подобную атрибутику.

Но такая информационная защита может работать и априорно (без переживания негативного личного опыта), на основе тех знаний о должном и недолжном, которые заложены в сознание человека с детства. Например, у некоторых людей сознание совершенно закрыто от восприятия матерной брани и возможность внутреннего воздействия на них такой информации равна нулю[9], поскольку такая информация активно отторгается почти на физиологическом уровне (как неприятие тухлой пищи). У подавляющего же большинства людей такие защитные механизмы отсутствуют по очень большому спектру информационных угроз, а потому информационная безопасность требует активного участия государства в ее обеспечении.

С началом военных действий стало появляться смутное и не вполне оформившееся понимание масштаба информационных угроз, а потому государство предпринимает попытки борьбы с ними. Есть верное понимание, что эффективная борьба требует усилия в двух направлениях: формирование сознания на основе правильной ценностной иерархии и меры контроля и ограничения в отношении источников информации. Но делается это все на скорую руку и без глубокого осмысления, поэтому пока усилия в этих направлениях напоминают хаотичные телодвижения человека, который, почувствовав угрозу, начинает размахивать руками, пытаясь от нее защититься. А надо не махать руками, а прицельно стрелять.

Указ Президента РФ от 09.11.2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» можно назвать одним из шагов на пути к обеспечению информационной безопасности. Но пока это шаг человека, который пытается найти верное направление, но движется в темноте на ощупь. Проиллюстрируем сказанное всего одним примером. Если в п. 5 этого Указа первой ценностью провозглашается жизнь, а по статистике за 2023 г. в России сделано 467 тысяч абортов[10], значит «жизнь», о которой говорится в Указе, всего лишь термин,

---

[9] Возможно лишь внешнее воздействие, от которого человеку становится противно, как от неприятного запаха или вида разлагающегося трупа, например.

[10] URL: https://www.kommersant.ru/doc/7497492 (дата обращения: 31.03.2025).

не наполненный содержанием. В контексте информационной безопасности можно предложить рассмотреть два сценария: 1) государство будет активно защищать в информационном пространстве право женщин на прерывание беременности; 2) государство будет активно участвовать в информационном противодействии такому решению беременных женщин. Какой из этих сценариев соответствует интересам обеспечения информационной безопасности?

В заключение — краткие соображения по второму направлению обеспечения информационной безопасности: контроль информационных потоков и ответственность за распространение деструктивной информации. В этом направлении успех возможен лишь в том случае, если:

1) информационные ресурсы физически находятся в пределах досягаемости российских правоохранительных органов;

2) существует возможность блокировки информации из источников, находящихся вне такого контроля;

3) для владельцев информационных ресурсов, которые сами не распространяют информацию, устанавливается обязанность самоцензуры всех материалов, которые размещены на той или иной информационной платформе.

БИБЛИОГРАФИЯ

1. *Ефремова М. А.* Информационная безопасность как объект уголовно-правовой охраны // Информационное право. — 2014. — № 5.
2. *Гумилев Н. С.* Полное собрание сочинений : в 10 т. — М. : Воскресенье, 1998. — Т. 3 : Стихотворения. Поэмы / ред. колл. : Н. Н. Скатов (гл. ред.) [и др.] ; РАН. Ин-т рус. лит. (Пушк. дом.).
3. Комментарий к Уголовному кодексу Российской Федерации : в 4 т. — М. : Юрайт, 2017. — Т. 3 : Особенная часть / отв. ред. В. М. Лебедев.
4. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. В. Бриллиантова : в 2 т. — 2-е изд. — М. : Проспект, 2015. — Т. 2.
5. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под ред. А. И. Чучаева. — 3-е изд., испр. и доп. — М. : Контракт, 2011.
6. *Кузьмин В. П.* Понятие и юридическая сущность информации // Информационное право. — 2009. — № 2.
7. *Чеботарева А. А.* Обеспечение информационной безопасности личности в Интернете: история и проблемы развития законодательства // История государства и права. — 2010. — № 11.