DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

ГОСУДАРСТВЕННАЯ БЕЗОПАСНОСТЬ

Карчевский Н.В.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: *В работе предпринимается попытка сформулировать основные требования к содержанию уголовно-правовой охраны общественных отношений в сфере информатизации. Обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уголовно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения этой системы предлагается использовать термин «информационная безопасность». Субъект находится в состоянии информационной безопасности тогда, когда эффективность его деятельности обеспечена полной, достоверной и достаточной для принятия решений информацией. Такое состояние достигается социальной активностью в трех взаимосвязанных группах общественных отношений, представляющих собой структурные элементы информационной безопасности: общественные отношения в сфере использования информационных технологий, в сфере обеспечения доступа к информационному ресурсу и в сфере формирования информационного ресурса. При этом, общественная опасность посягательств на информационную безопасность не является самостоятельной, зависит от социальной значимости тех отношений, в пределах которых возникает информационная потребность. Предлагаются основные направления совершенствования законодательства об уголовной ответственности за преступления в сфере информационных технологий, а также в сфере ограниченного доступа к информации. Обосновывается нецелесообразность широкого применения средств уголовной юстиции в сфере формирования информационного ресурса.*

Ключевые слова: *Юриспруденция, информатизация, информационная безопасность, преступление, информационные технологии, ограниченный доступ к информации, формирование информационного ресурса, эффективность уголовно-правовой охраны, злоупотребление уголовным правом, оптимизация законодательства об уголовной ответств.*

Abstract: *In this work the author attempts to formulate the key requirements for providing criminal legal protection of the public relations in the area of informatization. The system of criminal legal protection of public relations that is responsible for meeting the informational demand and is intended for providing the criminal legal stimulation of the positive, and minimization of the negative social consequences of informatization can be referred to as ''information security''. The subject remains in the state of information security when the effectiveness of their activity is provided with accurate and sufficient information for making a decision. This state can be achieved by the social activity in three interlinked groups of social relations that represent the structural elements of information security: public relations in the sphere of use of information technologies; in the sphere of providing access to information resource; in the sphere of creating an information resource. At the same time the public danger of infringing on the information security is not independent, but rather depends on the social significance of the relations within which the information demand emerges. The author proposes the main directions for improving the legislation on the criminal liability for the crimes in the area of information technologies, as well as the sphere of limited access of information. The bases are provided for the unreasonableness of a wide implementation of means of criminal justice in the sphere of forming an information resource.*

Keywords: *Jurisprudence, Informatization, Information security, Crime, Information technologies, Limited access to information, Forming of information resource, Effectiveness, Abuse of criminal law, Optimization of legislation on criminal liability.*

Процессы информатизации и компьютеризации во многом определяют содержание современных социальных трансформаций. Подчиняясь диалектическому закону, они не являются однозначными. Вместе с очевидным расширением возможностей человека в удовлетворении информационных потребностей широкое распространение информационных технологий привело к появлению и развитию целого комплекса негативных социальных тенденций. При этом развитие форм и видов противоправного при-

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

менения современных компьютерных технологий, так называемая киберпреступность, является далеко не единственным последствием взрывной информатизации общества. Значительным потенциалом общественной опасности характеризуются также: чрезмерная капитализация информационного пространства; развитие возможностей манипуляции общественным сознанием в политической сфере; формирование сверхмощных баз персональных данных, представляющих опасность тотального контроля над личностью; рост уровня идеологической уязвимости политических систем из-за наличия глубоких социальных конфликтов, которые могут быть задействованы путем использования информационных технологий; интеллектуальная и духовная деградация общества и т.д. Тут следует отметить, что по оценкам ведущих экспертов основной тенденцией развития информационных технологий в последующие 5 лет станет кардинальное увеличение объема данных, передаваемых при помощи современных средств коммуникации [1]. Данный прогноз позволяет обоснованно предполагать, что перечисленные негативные последствия информатизации проявятся в скором времени более рельефно. Очевидно и то, что общественная опасность злоупотреблений в сфере применения информационных технологий будет возрастать. Сказанное подчеркивает актуальность исследований в сфере уголовно-правового обеспечения процессов информатизации.

В данной работе предпринимается попытка сформулировать основные требования к содержанию уголовно-правовой охраны общественных отношений в сфере информатизации.

Первым должен быть решен вопрос объекта уголовно-правовой охраны в сфере информатизации. Какие общественные отношения должны охранять нормы права, для того, чтобы обеспечивать развитие положительных и минимизацию негативных социальных последствий информатизации? Очевидно, что речь идет об общественных отношениях, в пределах которых обеспечивается реализация информационной потребности граждан, общества или государства. Именно необходимость реализации возрастающей информационной потребности вызвала в своё время появление речи, письма и технологий книгопечатанья, стимулировала развитие радио и телевидения и обуславливает сегодня постоянное совершенствование и расширение сферы применения современных компьютерных технологий. Поэтому правовое регулирование и охрана именно этих отношений, отношений в сфере реализации информационной потребности, может обеспечить предупреждение негативных последствий информатизации.

Для обозначения системы общественных отношений, направленных на обеспечение реализации информационной потребности граждан, общества или государства предлагается использовать термин *«информационная безопасность»*. Информационную безопасность субъекта следует считать обеспеченной тогда, когда он имеет возможность получать полную, достоверную и достаточную для принятия эффективных решений информацию. Такое состояние достигается социальной активностью в трех взаимосвязанных группах общественных отношений, представляющих собой структурные элементы информационной безопасности: общественные отношения в сфере использования информационных технологий, в сфере обеспечения доступа к информационному ресурсу и в сфере формирования информационного ресурса. В пределах первой группы выполняется задание обеспечения функционирования эффективных средств информационной деятельности, в пределах второй – обеспечивается возможность субъектов получать беспрепятственный доступ к необходимым информационным ресурсам, а в пределах третьей – обеспечивается формирование информационного ресурса, который отвечает потребностям субъектов [5].

Определенного внимания требует вопрос о том, насколько обосновано названные группы общественных отношений называть системой, представляют ли они, в связи с этим, единый объект уголовно-правовой охраны? Рассмотрение данных общественных отношений как самостоятельной системы обусловлено двумя факторами: во-первых, взаимозависимость названных групп общественных отношений; во-вторых, единая для всех трёх групп специфика социальной значимости, свидетельствующая о необходимости применения мер правового регулирования.

Функционирование и эффективность каждого из элементов системы информационной безопасности обусловлены другими её элементами. Предоставление доступа к информации не имеет смысла без формирования информационного ресурса и является неэффективным без использования информационных технологий. Значение формирования информационного ресурса определяется возможностью дальнейшего доступа к нему и обеспечивается путем использования информационных технологий. Функционирование информационных технологий приобретает социальное значение именно как средства доступа и формирования информационных ресурсов.

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

Социальная значимость как формирования информационного ресурса, так и предоставления доступа к информации, а также использования информационных технологий определяется значением тех общественных отношений, в пределах которых возникает информационная потребность. То есть, общей чертой отношений информационной безопасности, является то, что целесообразность их уголовно-правовой охраны, определяются социальной значимостью тех общественных отношений, в пределах которых возникает информационная потребность. Именно значимость последних определяет значимость отношений информационной безопасности, а также целесообразность и интенсивность соответствующих мер правового регулирования. Например, значимость доступа к информации и, как следствие, необходимость его правового регулирования не является самостоятельной и определяется важностью той деятельности, для осуществления которой нужен доступ. Последствия незаконного получения доступа к информации определяются не самим фактом незаконного ознакомления с определенной закрытой информацией, а содержанием тех отношений, в пределах которых возникла потребность ограничения доступа. Опасность нарушения функционирования определенной компьютерной сети определяется важностью заданий, для которых она используется, именно последние выступают критерием обоснованности применения соответствующих средств уголовной юстиции.

Отметим, что термин «информационная безопасность» достаточно широко применяется в информатике и обозначает, как правило, комплекс мероприятий по обеспечению защиты информации от уничтожения или незаконного доступа; совокупность организационных, программных и технических средств обеспечивающих целостность, конфиденциальность и доступность данных. Тем не менее, применение его в юридическом контексте для обозначения самостоятельного объекта уголовно-правовой охраны, также представляется обоснованным. Вызвано это достижением соответствующими отношениями социального значения, требующего применения средств уголовной юстиции. Можно говорить о том, что современные тенденции информатизации позволяют рассматривать информационную безопасность как в узком смысле (обеспечение защиты информации) так и в широком – обеспечение реализации социальной информационной потребности.

Итак, *обеспечение уголовно-правового стимулирования положительных и минимизации негативных социальных последствий информатизации, предполагает определение в качестве самостоятельного объекта уголовно-правовой охраны системы общественных отношений, обеспечивающих реализацию информационной потребности. Для обозначения этой системы предлагается использовать термин «информационная безопасность», её структуру составляют отношения в сфере формирования информационного ресурса, обеспечения доступа к информации, а также отношения в сфере использования информационных технологий. Социальная значимость отношений информационной безопасности, а следовательно и целесообразность их уголовно-правовой охраны, определяются значимостью тех отношений, в пределах которых возникает информационная потребность*. Вместе с тем, обеспечение уголовно-правовой охраны каждой из обозначенных групп имеет определённую специфику.

Начнём с отношений *в сфере использования информационных технологий*. Основная правовая проблема здесь – обеспечение нормативно-правовой базы противодействия так называемым «компьютерным» преступлениям. С учётом высказанных ранее положений, сформулируем следующее положение: критерием отнесения определённых деяний к преступлениям в сфере использования информационных технологий следует считать вред, причиняемый той социально значимой деятельности, для осуществления которой применяется компьютерная техника. Очевидно, что уничтожение информации, обрабатываемой в компьютерной системе, опасно настолько, насколько социально значимой является задача, для решения которой используется определенный компьютер. Тем не менее, законы об уголовной ответственности некоторых государств не учитывают такой специфики. Так, судя по решению, принятому украинским законодателем, утечка, потеря, подделка, блокирование информации, нарушение установленного порядка ее маршрутизации или искажение процесса ее обработки (ст. 361, 362 УК Украины) признаются общественно-опасными сами по себе. Лишь на уровне квалифицирующих признаков мы встречаем зависимость уголовной ответственности от наступления «существенного вреда». Аналогичные выводы могут быть сделаны и относительно содержания ст. ст. 272 и 273 УК РФ; ст. 268 УК Польши; ст. 9с Главы 4 УК Швеции. Не лишены указанного недостатка и положения Конвенции о киберпреступности. Подобная ситуация приводит к вполне ожидаемым проблемам: из-за отсутствия в законодательных определениях «компьютерных» преступлений четких критериев общественной опасности под уголовно-правовой запрет и, соответственно, в сферу действия уголовной юстиции попадают не только деяния, которые действительно

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

являются общественно опасными, но и не являющиеся таковыми. Это приводит к существенному снижению эффективности уголовно-правового противодействия данным преступлениям[1].

Исправление ситуации в первую очередь предусматривает включение в диспозиции соответствующих уголовно-правовых норм четких положений относительно критериев общественной опасности посягательств. Одним из возможных и наиболее оптимальных решений является обращение к законодательным конструкциям, свойственным преступлениям с производными последствиями. Структура объективной стороны преступлений в сфере использования компьютерной техники должна включать: 1) основные последствия – различные формы нарушения информационных отношений, выступающих непосредственными объектами (уничтожение, блокирование, нарушение целостности информации и т.д.); 2) производные последствия – нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц. Лишь при наличии совокупности таких последствий совершенное посягательство следует считать преступлением в сфере использования информационных технологий.

В самом общем смысле, правовое регулирование *отношений обеспечения доступа к информации* представляет собой поиск баланса между двумя группами противоположных социальных интересов: с одной стороны – интересов определенных субъектов в ограничении доступа к информации, а с другой – интересов определенных субъектов в получении информации. Поэтому, сущность нарушений информационной безопасности в данной сфере заключается в том, что нарушение реализации информационной потребности обусловлено или нарушением установленного режима доступа к определенному ресурсу, или неправомерным ограничением доступа к определенной информации. Следует отметить, что отношения доступа к информации весьма продолжительный период времени регулировались правом и охранялись уголовным законом, хотя до определенного уровня технологического развития не имели самостоятельного значения. С компьютеризацией общества, появлением Интернета произошел взрывной рост количественных и качественных показателей накопления и использования информации во всех сферах социальной жизни и жизни отдельных граждан. Современные информационные технологии радикально изменили структуру и формы общения. Сегодня сама форма организации общества, его эффективность прямо зависят от обеспечения достоверности информации, сохранения сформированных потоков данных и скорости их передачи. Если еще сто лет тому назад посягательства на информационные отношения преимущественно не рассматривались как такие, что характеризуются существенной общественной опасностью, то сегодня есть все основания ставить знак равенства между информационной безопасностью и безопасностью общества в целом. Нужно признать, что уголовным законодательством такие изменения остались скорее незамеченными. *Нормы об уголовной ответственности за нарушения ограниченного доступа к информации рассредоточены, встречаются в различных законах об уголовной ответственности*, хотя очевидно, что интенсивность уголовно-правовой охраны отношений в сфере ограниченного доступа к информации должна определяться не видом информации (государственная тайна, коммерческая, тайна усыновления и т.д.), а содержанием наступивших последствий.

Таким образом, имеющаяся в действующем законодательстве система норм об ответственности за преступления в сфере информационной безопасности должна рассматриваться с позиций ее оптимизации. Очевидно, что в ходе ее совершенствования *должен решаться вопрос о целесообразности, обоснованности и пределах замены имеющейся рассредоточенной системы специальных уголовно-правовых запретов такими нормами, которые бы обеспечивали охрану более широких сегментов отношений информационной безопасности. Есть смысл отказаться от чрезмерной детализации уголовно наказуемых видов нарушений ограниченного доступа к информации.* Б.Г. Розовский четко зафиксировал одну из основных закономерностей развития уголовного законодательства: от первичного понятия преступления, которое по содержанию было примитивно простым и предусматривало оценку опасности посягательства на конкретный материализованный предмет – кража коня, кража оружия, лишения глаза и тому подобное, к обобщениям (например, кража не коня, а кража скота), отказу от предметной индивидуализации, появлению видовых обобщений (кража, мошенничество). Такой подход позволяет автору критически оценить современные законотворческие процессы в уголовном праве. Б.Г. Розовский обосно-

[1] Данный вывод был доказан в ходе исследования практики применения украинского законодательства об уголовной ответственности [3]. Близость указанных законодательных формулировок «компьютерных» преступлений, содержащихся в УК иных государств, позволяет предположить наличие аналогичных проблем эффективности уголовно-правового противодействия.

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

ванно доказывает, что в последнее время происходит обратный процесс – декристаллизация, возвращение в варварство: однотипные по своей сути преступления все чаще дифференцируются [8, с. 30-31].

В пользу отказа от разветвленной системы норм об ответственности за преступления в сфере ограниченного доступа к информации свидетельствует и специфика современных процессов в сфере информатизации. Дальнейшее развитие будет заключаться в объединении разрозненных источников и ресурсов информации, используемых в разнообразных сферах человеческой деятельности (образование, здравоохранение, торговля, предоставление услуг и т. д.), в одном информационном поле. Интеграция информационных ресурсов обеспечивает существенное повышение эффективности их использования, именно поэтому она и является основным направлением процессов информатизации общества. Наиболее ярко этот процесс может быть продемонстрирован на примере развития систем информационного обеспечения правоохранительной деятельности. Так, в процессе выполнения задач относительно выявления и раскрытия преступлений, розыска лиц, которые их совершили, работники ОВД нуждаются в информации относительно состояния здоровья отдельных лиц, их образовании и т. д. Что происходило раньше. Посылались письменные запросы в наркологический и психоневрологический диспансеры, детские лечебные заведения, учреждения образования, военкоматы и т. д., там осуществлялся поиск нужной карточки в архиве, после этого по почте посылался ответ. Для того, чтобы дать оценку эффективности этого процесса в контексте противодействия преступности, комментарии излишни. В настоящее время эта информация формируется в единый банк данных.

Понятно, что в масштабе государства, при принятии соответствующих управленческих решений, разработке программ и перспективных планов развития, формировании законотворческой политики централизация всей информации, относительно процессов, происходящих в обществе, крайне важная и необходима. Интеграция информационных ресурсов происходит и в коммерческой сфере. Например, торговые сети, используя разнообразные средства, осуществляют накопление и анализ больших объемов информации для обеспечения более эффективных продаж и рекламы.

В процессе создания таких систем неминуемо возникнет потребность в четкой регламентации порядка их функционирования, а также единой системе ответственности за нарушения в данной сфере. То есть имеющаяся необходимость интеграции информационных ресурсов непременно приведет к унификации правового регулирования и охраны соответствующих общественных отношений. Следовательно, приведенное выше предложение относительно отказа от разветвленной системы специальных норм и их замены общими, полностью отвечает тенденциям информатизации общества. Итак, целесообразным представляется отказ от разветвленной системы норм, предусматривающих ответственность за фактически одинаковые деяния, но относительно информации с ограниченным доступом разных видов. При этом, несомненно, есть смысл в сохранении ряда специальных запретов, но только тех, которые характеризуются существенно большей общественной опасностью (например, государственная измена или шпионаж).

Наконец, об уголовно-правовой охране общественных отношений в сфере формирования информационного ресурса. Специфика здесь заключается в том, что *включение в социальный дискурс информации, дезориентирующей субъектов социального бытия, оказывает манипулятивное влияние на общественное сознание и может привести к совершению членами социума деяний, являющихся опасными для его стабильности и развития*. Например, общественная опасность публичных призывов к свержению конституционного строя заключается в том, что определенные субъекты, нуждающиеся в общественно-политической информации о возможностях развития государства, будут введены в заблуждение относительно целесообразности решения неотложных социальных проблем путем насилия. В свою очередь наличие значительного количества таких субъектов будет представлять угрозу национальной безопасности государства.

Следует отметить, что проблема уголовно-правового обеспечения формирования информационных ресурсов не является новой. Уголовные законодательства подавляющего числа государств содержат нормы об ответственности за: призывы к насильственному свержению конституционного строя; умышленные действия, направленные на разжигание национальной, расовой или религиозной вражды и ненависти, на унижение национальной чести и достоинства, или обиды чувств граждан в связи с их религиозными убеждениями; публичные призывы к совершению террористического акта; призывы к совершению действий, которые угрожают общественному порядку; изготовление или распространение произведений, которые пропагандируют культ насилия и жестокости; изготовление, сбыт и распространение порнографических предметов; публичные призывы к геноциду и т.д.

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

Однако, в современных условиях, условиях повышения интенсивности массовой коммуникации, угрозы, обусловленные нарушениями в сфере формирования информационного ресурса, гораздо глубже и сложнее. Уже сегодня специалисты отмечают, что средства массовой коммуникации все чаще вводят своего потребителя в состояние, при котором действуют механизмы и неписаные законы личного обогащения, отчужденности, безразличия к обществу, все более развращают его насилием, пропагандой наркотиков, алкоголя, преступности и безнаказанности [7, с. 84]. Обосновывается, что одним из факторов формирования мотивации противоправного поведения несовершеннолетних является деструктивное влияние СМИ [2, с. 70]. В.И. Данилов-Данильян и И.Е. Рейф отмечают, что, обеспечив большинству населения высокий уровень благосостояния, развитая рыночная экономика почти ничего не сделала для повышения культурного уровня рядового американца или европейца. Напротив, выгодным оказалось «промывание мозгов» с помощью рекламы и других пиартехнологий, чтобы упростить его духовные потребности и снизить культуру к субкультуре с ее кинобоевиками, любовно-эротичными, детективными романами, попсовой музыкой, всяческими «диснейлендами», клубами фитнесса, коммерческим спортом, казино и т. д. [3] В конце концов, современная массовая коммуникация, ориентированная в первую очередь на философию потребления, может привести к духовному и интеллектуальному вырождению общества [6].

При этом обоснованно прогнозировать, что ожидаемое увеличение интенсивности массовой коммуникации существенно обострит данные угроз, приведет к тому, что их развитие ускорится. Зафиксировав, настолько тревожные социальные тенденции, рассмотрим, какие средства уголовно-правовой охраны могут быть использованы для их предупреждения и минимизации последствий. Наиболее распространенным и, возможно, исторически первым средством противодействия общественно опасным проявлениям в сфере формирования информационного ресурса является контроль за содержанием сообщений и ограничение доступа к ним. Именно к таким средствам следует относить упомянутые ранее нормы действующего уголовного законодательства. Однако эти уголовно-правовые запреты нельзя рассматривать как целостную систему, они представляют собой законодательную реакцию на наиболее опасные проявления нарушений формирования информационного ресурса, относящиеся к разнообразным сферам социального бытия: национальной безопасности, противодействию расовой неприязни и ксенофобии, общественной безопасности, морали и т. д. Возможно, установленные общественно опасные последствия современных процессов формирования информационного поля требуют уголовно-правовых запретов более широкого спектра действия? Таких, которые бы обеспечивали противодействие включению любого негативного контента в общественный информационный ресурс, исключали бы возможность манипулирования общественным сознанием? Так, с целью предотвращения негативного влияния содержания, интернет-ресурсов Председатель правительства РФ Дмитрий Медведев подписал постановление «О единой автоматизированной информационной системе „Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети „Интернет“, содержащих информацию, распространение которой в Российской Федерации запрещено“ [13]. Целесообразность данного подхода находит определенное подтверждение и в работах учёных. Например, О. Бугера обращает внимание на необходимость строгого соблюдения требований ограничения зрительской аудитории и индексации сообщений СМИ в зависимости от содержания [2, с. 71]. Н.А. Савинова предлагает предусмотреть уголовную ответственность за такие посягательства как «умышленные воздействия на сознание», «неосторожные воздействия на сознание», «распространение унизительной для государства медиа продукции», «использование скрытых средств влияния на сознание в средствах массовой информации» [11, с. 252-299]. Следовательно, возможно, уголовное законодательство необходимо дополнить нормами об ответственности за несоблюдение правил индексации контента, или об ответственности провайдеров телекоммуникационных услуг за трансляцию общественно вредного контента, или об ответственности выпускающих редакторов СМИ за распространения сведений, которые вызывают наступление общественно опасных последствий?

Ответ на поставленные вопросы является негативным. И дело не только в том, что усиление государственного контроля за деятельностью средств массовой информации путем включения дополнительных уголовно-правовых средств потенциально опасно свертыванием процессов демократизации. Попытка сформулировать подобные новеллы приведет к ожидаемой проблеме: принципиально невозможно сформулировать четкое и операциональное определение для обозначения тех сведений, включение которых в информационное поле следует считать общественно опасным. Весьма пробле-

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

матичной будет и попытка четкого, а именно такое необходимо для уголовно-правовой нормы, определения общественно опасных последствий. Такая ситуация с необходимостью приведет к формулировке уголовно-правового запрета на основе оценочных понятий, что в свою очередь *создаст необоснованный риск злоупотреблений уголовным правом.*

Кроме того, *распространение глобальных информационных технологий (Интернет, сети спутникового вещания) вообще делает все менее эффективными методы, основывающиеся на ограничении или запрете распространения определенной информации*. Например, тотальный мониторинг Интернета, по мнению западных специалистов в вопросах информационной безопасности, не может помочь в борьбе с экстремизмом даже теоретически. Плотность современных информационных потоков настолько большая, что даже для выборочной своевременной проверки отдельных информационных источников понадобится такое количество специалистов, которое в несколько раз превышает экономически обоснованную численность всех правоохранительных органов государства [9]. Стоит согласиться и с тем, что вертикальная регуляторная схема, срабатывающая относительно минимизации угроз, связанных с распространением вредоносного контента в традиционных масс-медиа, не действует в условиях интерактивности и глобальности [4]. Определенным подтверждением сказанному является тот факт, что сразу же после начала работы упомянутого ранее Реестра доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети „Интернет“, содержащих информацию, распространение которой в Российской Федерации запрещено, в российском сегменте сети появились многочисленные публикации, содержащие предложения по обходу вводимых запретов [12]. Сказанное, конечно же, не означает, что политика государственного ограничения интернет-контента является неэффективной, излишней. Такие ограничения необходимы и будут особенно актуальны с учетом имеющегося прогноза увеличения интенсивности массовой коммуникации. Однако, приведенные положения достаточно чётко свидетельствуют о том, что включение в этот механизм государственного контроля уголовно-правовых средств, средств представляющих по своей сути ultima ratio правового регулирования, является излишним.

Итак, очевидно, что *комплекс вопросов, связанных с правовым регулирование процессов формирования информационного ресурса, имеет свое решение преимущественно за пределами уголовно-правового поля.* Именно неэффективность традиционных средств противодействия негативным информационным воздействиям позволяет специалистам делать вывод о том, что осознавать серьезность проблем, которые создает современное информационное поле, вовсе не означает только наказывать, запрещать, фильтровать, закрывать, конфисковывать. Обращается внимание на такие меры предупреждения негативного информационного влияния, как воспитание уважения к правам других людей и умению отстаивать свои собственные, родительский контроль, ограничение виртуальных социальных контактов, развитие навыков критического восприятия информации, поступающей из медийного пространства [10].

Таким образом, основные требования к содержанию уголовно-правовой охраны общественных отношений в сфере информатизации заключаются в следующем:

1. объектом уголовно-правовой охраны в данной сфере следует считать информационную безопасность – систему общественных отношений, в пределах которых обеспечивается реализация информационной потребности граждан, общества, государства;
2. указанная система состоит из трёх элементов – отношения в сфере формирования информационного ресурса, отношения в сфере обеспечения доступа к информации, отношения в сфере использования информационных технологий;
3. целесообразность уголовно-правовой охраны информационной безопасности, определяются значимостью тех отношений, в пределах которых возникает информационная потребность;
4. повышение эффективности уголовно-правовой охраны отношений в сфере использования информационных технологий предполагает включение в соответствующие законы четких положений относительно критериев общественной опасности посягательств, обеспечивающих применение средств уголовной юстиции только в тех случаях, когда имеет место обусловленное посягательством в сфере информационных технологий существенное нарушение отношений в сфере реализации прав и свобод отдельных физических лиц, государственных или общественных интересов, деятельности юридических лиц;
5. система норм об уголовной ответственности за преступления в сфере ограниченного доступа к информации требует оптимизации, в ходе ее совершенствования должен решаться вопрос о

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

целесообразности, обоснованности и пределах замены имеющейся рассредоточенной системы специальных уголовно-правовых запретов такими нормами, которые бы обеспечивали охрану более широких сегментов отношений информационной безопасности;

6. несмотря на то, что количественные и качественные показатели информатизации позволяют прогнозировать усиление развития негативных социальных последствий в сфере формирования информационных ресурсов, расширение уголовно-правовых средств в данной сфере, дополнение уголовного законодательства новыми нормами об ответственности за распространение «общественно опасной информации», является нецелесообразным из-за прогнозируемой неэффективности таких норм, непринадлежности решений данных социальных проблем к уголовно-правовому полю.

Библиография:

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016. [Electronic resource] // Cisco Systems, Inc. Official site. – Mode of access: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.
2. Бугера О. Засоби масової інформації: проблема вдосконалення діяльності щодо запобігання протиправної поведінки неповнолітніх / О. Бугера // Підприємництво, господарство і право. – 2005. – № 7. – С. 70–73.
3. Данилов-Данильян В. Что может и чего не может рыночная экономика / В. Данилов-Данильян, И. Рейф // Наука и жизнь. – 2010. – № 9. – С. 2–8.
4. Зернецкая О. Интернет-ловушка для молодежи [Электронный ресурс] / О. Зернецкая // Зеркало недели. – 2007. – № 11. – Режим доступу: http://zn.ua/articles/49507.
5. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський – Луганськ, 2011. – 538 с.
6. Кендюхов О. Суспільство споживання як національна трагедія України [Електронний ресурс] / О. Кендюхов // Дзеркало тижня. – 2011. – № 1. – Режим доступу: http:// dt.ua/articles/73290.
7. Коваленко В. В. Сучасна масова комунікація: носій добра чи криміногенний фактор? / В. В. Коваленко // Право України. – 2008. – № 4. – С. 84–89.
8. Криммінальне право (Особлива частина): підручник / за ред. О. О. Дудорова, Є. О. Письменського. Т. 1 – Луганськ : видавництво «Елтон -2», 2012. – 780 с.
9. Паньо Е. Сито со слишком большими дырочками [Электронный ресурс] / Е. Паньо, Т. Паньо // Зеркало недели. – 2006. – № 24. – Режим доступу: http://zn.ua/articles/47040.
10. Приходько О. Дети в Интернете: реальные риски виртуальных погружений [Электронный ресурс] / О. Приходько // Зеркало недели. – 2009. – № 12. – Режим доступа: http://zn.ua/articles/56562.
11. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія / Н. А. Савінова. – К. 2012. – 340 с.
12. Серветтаз Е. Интервью: Как обойти запрет на сайты из «черного списка» Роскомнадзора / Елена Серветтаз [Электронный ресурс] // RFI русский. – 13 Ноября 2012 г. – Режим доступа: http://www.russian.rfi.fr/rossiya/20121113-intervyu-kak-oboiti-zapret-na-saity-iz-chernogo-spiska-roskomnadzora
13. Соседский опыт. Новости для Интернета [Электронный ресурс] // Зеркало недели. Украина – 2 ноября 2012 г. – Режим доступа: http://zn.ua/LAW/sosedskiy_opyt_novosti_dlya_interneta-111534.html.

References (transliterated):

1. Bugera O. Zasobi masovoï informatsiï: problema vdoskonalennya diyal'nosti shchodo zapobigannya protipravnoï povedinki nepovnolitnikh / O. Bugera // Pidpriємnitstvo, gospodarstvo i pravo. – 2005. – № 7. – S. 70–73.
2. Danilov-Danil'yan V. Chto mozhet i chego ne mozhet rynochnaya ekonomika / V. Danilov-Danil'yan, I. Reif // Nauka i zhizn'. – 2010. – № 9. – S. 2–8.
3. Zernetskaya O. Internet-lovushka dlya molodezhi [Elektronnyi resurs] / O. Zernetskaya // Zerkalo nedeli. – 2007. – № 11. – Rezhim dostupu : http://zn.ua/articles/49507.
4. Karchevs'kii M. V. Kriminal'no-pravova okhorona informatsiinoï bezpeki Ukraïni : monografiya / M. V. Karchevs'kii – Lugans'k, 2011. – 538 s.
5. Kendyukhov O. Suspil'stvo spozhivannya yak natsional'na tragediya Ukraïni [Elektronnii resurs] / O. Kendyukhov // Dzerkalo tizhnya. – 2011. – № 1. – Rezhim dostupu: http:// dt.ua/articles/73290.
6. Kovalenko V. V. Suchasna masova komunikatsiya: nosii dobra chi kriminogennii faktor? / V. V. Kovalenko // Pravo Ukraïni. – 2008. – № 4. – S. 84–89.
7. Pan'o E. Sito so slishkom bol'shimi dyrochkami [Elektronnyi resurs] / E. Pan'o, T. Pan'o // Zerkalo nedeli. – 2006. – № 24. – Rezhim dostupu: http://zn.ua/articles/47040.

DOI: 10.7256/1811-9018.2015.2.8115
При цитировании этой статьи сноска на doi обязательна

8. Prikhod'ko O. Deti v Internete: real'nye riski virtual'nykh pogruzhenii [Elektronnyi resurs] / O. Prikhod'ko // Zerkalo nedeli. – 2009. – № 12. – Rezhim dostupa: http://zn.ua/articles/56562.
9. Savinova N. A. Kriminal'no-pravove zabezpechennya rozvitku informatsiinogo suspil'stva v Ukraïni: teoretichni ta praktichni aspekti : monografiya / N. A. Savinova. – K. 2012. – 340 s.
10. Servettaz E. Interv'yu: Kak oboiti zapret na saity iz «chernogo spiska» Roskomnadzora / Elena Servettaz [Elektronnyi resurs] // RFI russkii. – 13 Noyabrya 2012 g. – Rezhim dostupa: http://www.russian.rfi.fr/rossiya/20121113-intervyu-kak-oboiti-zapret-na-saity-iz-chernogo-spiska-roskomnadzora